S. HRG. 113–781

THE LOCATION PRIVACY PROTECTION ACT OF 2014

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JUNE 4, 2014

Serial No. J–113–63

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE

97–739 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California	CHUCK GRASSLEY, Iowa, *Ranking Member*
CHUCK SCHUMER, New York	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	JEFF FLAKE, Arizona
MAZIE HIRONO, Hawaii	

KRISTINE LUCIUS, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

AL FRANKEN, Minnesota, *Chairman*

DIANNE FEINSTEIN, California	JEFF FLAKE, Arizona, *Ranking Member*
CHUCK SCHUMER, New York	ORRIN G. HATCH, Utah
SHELDON WHITEHOUSE, Rhode Island	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	JOHN CORNYN, Texas
MAZIE HIRONO, Hawaii	LINDSEY GRAHAM, South Carolina

ALVARO BEDOYA, *Democratic Chief Counsel*
ELIZABETH TAYLOR, *Republican Chief Counsel*

CONTENTS

JUNE 4, 2014, 2:35 P.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

ANSWERS

Page

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

THE LOCATION PRIVACY PROTECTION ACT OF 2014

WEDNESDAY, JUNE 4, 2014

UNITED STATES SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:35 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Al Franken, Chairman of the Subcommittee, presiding.

Present: Senators Franken, Blumenthal, and Flake.

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Chairman FRANKEN. This hearing will be called to order. Welcome to the Senate Judiciary Subcommittee on Privacy, Technology, and the Law. This is a hearing on my bill to protect sensitive location information, the Location Privacy Protection Act of 2014.

Three years ago, I held a hearing to look at how our laws were protecting the location information generated by smartphones, cell phones, and tablets. The first group that I heard from was the Minnesota Coalition for Battered Women. They told me that across Minnesota victims were being followed through so-called stalking apps specifically designed to help stalkers secretly track their victims.

I started investigating these stalking apps. Let me read you some of their websites.

Here is one called SPYERA. It says: "Most of the time if you think your spouse is being unfaithful, you are right." "[SPYERA] will be your spy in their pocket." "[Y]ou will need to sneak your spouse's phone and download it to their phone." "After the software is downloaded, you will be able to see where they are geographically. If your husband is in two counties over from where you live, SPYERA will tell you that." And, of course, "husband" can mean "wife" or "ex" or whatever you want to put in there.

Here is another. This is from FlexiSPY. "FlexiSPY gives you total control of your partner's phone without them knowing it—See exactly where they are, or were, at any given date and time."

Here is another quote that has since been taken down: "Worried about your spouse cheating? Track EVERY text, EVERY call and EVERY move they make using our EASY Cell Phone Spy Software."

These apps can be found online in minutes. And abusers find them and use them to stalk thousands of women around the country.

The Minnesota Coalition for Battered Women submitted testimony about a northern Minnesota woman who was the victim of domestic violence—and the victim of one of these stalking apps. This victim had decided to get help. And so she went to a domestic violence program located in a county building. She got to the building, and within 5 minutes, she got a text from her abuser asking her why she was in the county building. The woman was terrified. And so an advocate took her to the courthouse to get a restraining order. As soon as she filed for the order, she got a second text from her abuser asking her why she was at the county courthouse and whether she was getting a restraining order against him. They later figured out that she was being tracked through a stalking app installed in her phone.

This does not just happen in Minnesota. A national study conducted by the National Network to End Domestic Violence found that 72 percent of victim services programs across the country had seen victims who were tracked through a stalking app or a standalone GPS device. Without objection, I will add to the record the accounts of a few other victims.

Here is one from a victim in Illinois. She was living in Kansas with her abuser. She fled to Elgin, Illinois, a town three States away. She did not know that the whole time her cell phone was transmitting her precise location to her abuser. He drove the 700 miles to Elgin. He tracked her to a shelter and then to the home of her friend, where he assaulted her and tried to strangle her.

Here is one from a victim in Scottsdale, Arizona. Her husband and she were going through a divorce. Her husband tracked her for over a month through her cell phone. Eventually, he murdered their two children in a rage.

In most of these cases, the perpetrator was arrested because it is illegal to stalk someone. But it is not clearly illegal to make and to market and to sell a stalking app. And so nothing happened to the companies making money off of the stalking. Nothing happened to the stalking apps.

My bill would shut down these apps once and for all. It would clearly prohibit making, running, and selling apps and other devices that are designed to help stalkers track their victims. It would let police seize the money that these companies make and use that money to actually prevent stalking. My bill will prioritize grants to the organizations that train and raise awareness around GPS stalking. And it would make the Department of Justice get up-to-date statistics on GPS stalking. That is a big deal, because the latest statistics we have from DOJ are from 2006, and at that point they estimated over 25,000 people were being GPS-stalked annually, back in 2006, and we know what smartphone technology has done since then.

But my bill does not protect just victims of stalking. It protects everyone who uses a smartphone, an in-car navigation device, or any mobile device connected to the Internet. My bill makes sure that if a company wants to get your location or give it out to others, they need to get your permission first.

I think that we all have a fundamental right to privacy: a right to control who gets your sensitive information and with whom they share it. Someone who has a record of your location does not just know where you live. They know where you work and where you drop your kids off at school. They know the church you attend and the doctors that you visit.

Location information is extremely sensitive. But it is not being protected in the way it should be. In 2010, the Wall Street Journal found that half of the most popular apps were collecting their users' location information and then sending it to third parties, usually without permission.

Since then, some of the most popular apps in the country have been found disclosing their users' precise location to third parties without their permission. And it is not just apps. The Nissan Leaf's on-board computer was found sending drivers' locations to third-party websites. OnStar threatened to track its users even after they canceled their service; they only stopped when I and other Senators called them out on this. And a whole new industry has grown up around tracking the movements of people going shopping—without their permission, and sometimes when they do not even enter a store.

The fact is, that most of this is totally legal. With only a few exceptions, if a company gets your location information over the Internet, they are free to give it to almost anyone they want.

My bill closes these loopholes. If a company wants to collect or share your information, it has to get your permission first and put up a post online saying what the company is doing with your data. Once a company is tracking you, it has to be transparent, or else it has to send you a reminder that you are being tracked.

Those requirements apply only to the first company getting location information from your device. For any other company getting large amounts of location data, all they have to do is put up a post online explaining what they are doing with that data.

That is it. These rules are built on existing industry best practices, and they have exceptions for emergencies, theft prevention, and parents tracking their kids. The bill is backed by the leading anti-domestic violence and consumer groups. Without objection, I will add letters to the record from the Minnesota Coalition for Battered Women, the National Center for Victims of Crime, the National Women's Law Center, the Online Trust Alliance, and Consumers Union—all in support of my bill. This bill is just common sense.

[The letters and stalking cases appear as submissions for the record.]

Chairman FRANKEN. Before I turn it over to my friend the Ranking Member, I want to make one thing clear. Location-based services are terrific. I use them all the time when I drive across Minnesota. They save time and money, and they save lives. Ninety-nine percent of companies that get your location information are good, legitimate companies.

And so I have already taken into account many of the industry concerns that I heard when we debated this bill last Congress: I have capped liability, I have made compliance easier. And if folks still have issues with the bill, I want to address them.

So, with that, I will turn it over to Senator Flake.

OPENING STATEMENT OF HON. JEFF FLAKE,
A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator FLAKE. Thank you, Mr. Chairman. Thank you again to the witnesses for being here. I know you have busy schedules, and I really appreciate you doing this.

I think we can all agree that stalking and domestic violence are serious concerns. That is why I was pleased to support the reauthorization of the Violence Against Women Act. I agree with those who will testify today, like Ms. Southworth of the National Network to End Domestic Violence and Detective Hill on the second panel, that domestic violence and stalking are serious problems that need to be addressed. I am not aware of any concerns that have been expressed about some of the sections of this bill, those that address the stalking apps and directing the Government to study GSP stalking and prioritize grants to educate law enforcement about this problem.

Having said that, there are sections of the bill that I think are still a bit concerning. The bill before us regulates the commercial collection of geolocation information. Some concerns have been raised about its effect on businesses and applications that use geolocation information to provide consumers with services that they now rely on.

I would like to enter into the record letters from the National Retail Federation and the Interactive Advertisement Bureau if that is okay.

Chairman FRANKEN. Without objection.

Senator FLAKE. Thanks.

[The letters appear as submissions for the record.]

Senator FLAKE. In our efforts to protect the privacy of Americans, which is extremely important, we have got to be careful not to stifle innovation in dynamic sectors of the economy. A lot of the concerns that have been expressed are about static regulations that deal with a dynamic sector of the economy, and we want to make sure that we do not hamper development of new products and technologies.

With that, I look forward to the witnesses. Thanks.

Chairman FRANKEN. Thank you, Senator Flake.

The first panel of witnesses has seated themselves. Thank you.

Bea Hanson is the Principal Deputy Director of the United States Department of Justice Office on Violence Against Women. Before joining the OVW, Ms. Hanson was director for emergency services and the chief program officer for Safe Horizon, a crime victims service organization in New York City. Ms. Hanson is a Minnesotan by birth and was raised in St. Paul.

Jessica Rich is the Director of the FTC's Bureau of Consumer Protection. During her time at the FTC, Ms. Rich has led major policy initiatives related to privacy, data security, and emerging technologies; overseen enforcement actions; and developed significant FTC rules. She also received the Chairman's Award in 2011 for her contributions to the FTC's mission.

Mark Goldstein is the Director of Physical Infrastructure Issues for the U.S. Government Accountability Office. He is a frequent

witness before Congress and served as senior staff member of the Senate Committee on Homeland Security and Governmental Affairs. He will testify about the two different studies that GAO conducted at my request on the subject of location privacy.

I would like to welcome you all. Thank you for appearing. Your written testimony will be made part of the record. You each have about 5 minutes for any opening remarks that you would like to make. We will start with Ms. Hanson.

STATEMENT OF BEA HANSON, PRINCIPAL DEPUTY DIRECTOR, OFFICE ON VIOLENCE AGAINST WOMEN, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Ms. HANSON. Thank you so much. Good afternoon, Chairman Franken, Ranking Member Flake, and members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice regarding stalking, mobile devices, and location privacy.

My name is Bea Hanson, and I am the Principal Deputy Director of the United States Department of Justice Office on Violence Against Women, or OVW. One key way that the Department of Justice has focused on strengthening the criminal justice response to stalking is through the implementation of the Violence Against Women Act, or VAWA.

Since the passage of VAWA in 1994, we have made significant strides in enhancing the criminal justice system's response to stalking, and Congress has been a strong partner in our national efforts to address this issue.

Since 1994, Congress has amended VAWA to address our growing understanding of this crime, adding stalking to the purpose areas of grant programs, broadening the Federal interstate stalking statute to protect victims of cyber stalking, and enhancing penalties for repeat stalking offenders. Just last year, in the most recent VAWA reauthorization, Congress closed a loophole in the Federal cyber stalking statute to permit Federal prosecutors to pursue cases where the offender and the victim both lived in the same State. Congress also amended the Jeanne Clery Campus Security Act to require that universities report crime statistics on incidents of stalking.

As you both know, stalking is a complex crime, and it continues to be missed, misunderstood, and very much underestimated. Incidents of stalking behavior, when considered separately, may seem relatively innocuous. However, stalking behavior tends to escalate over time, and it is often paired with or followed by sexual assault, physical abuse, or homicide, as Chairman Franken has pointed out. Its victims feel isolated, vulnerable, and frightened, and tend to suffer from anxiety, from depression, and from insomnia.

Results of the 2010 National Intimate Partner and Sexual Violence Survey, or NISVS, which was released by the Centers for Disease Control in late 2011, demonstrate the grave scope of this crime. Using a conservative definition of stalking, the survey found that 6.6 million people were stalked in the previous 12-month period and that 1 in 6 women and 1 in 19 men were stalked at some point in their lifetimes.

The survey report noted that, although anyone can be a victim of stalking, females were more than three times more likely to be stalked than males, and that young adults had the highest rates of stalking victimization.

The report also showed the too frequent nexus between stalking and intimate partner abuse. For the overwhelming majority of victims, the stalker is someone who is known to them—an acquaintance, a family member, or, most often, a current or former intimate partner. And the NISVS report confirmed that most stalking cases involve some form of technology. More than three-quarters of the victims reported having received unwanted phone calls, voice messages, and text messages; and roughly one-third of the victims were watched, followed, or tracked with a listening or other kind of device.

The report authors noted that their findings showed a higher percentage of stalking than previous national studies and hypothesized that this increase could be due to new technologies that make stalking behavior easier.

Technology has provided new tools for stalkers. For example, the rapid increased use of cellular phones in recent years has created a new market in malicious software that, when installed on mobile devices, allows perpetrators to intercept victims' communications without their knowledge or consent. Through the use of this software, perpetrators can read victims' e-mail and text messages, listen to their telephone calls, trace their movements, and turn on the microphone in their phone to record conversations occurring in the immediate surrounding area. And all this can be done remotely and surreptitiously.

A recent study conducted by the National Network to End Domestic Violence, supported by the Department of Justice Office for Victims of Crime, further suggests that technology-enhanced stalking, including the use of mobile devices, is neither novel nor rare. Of the more than 750 victims service agencies that responded, 72 percent reported helping victims who had been tracked by GPS either through a cell phone or a GPS device.

The findings from NISVS and other surveys underscore how critical it is that professionals who work with stalking victims understand the dynamics of stalking, particularly how stalkers use technology. We know that stalking is often a precursor to other forms of violence. Because stalking can be challenging to recognize, OVW grant programs support specialized training for police, prosecutors, and others to ensure that comprehensive services are available to victims.

We also fund a number of training and technical assistance projects that target the intersection of technology and the crimes of stalking, sexual assault, domestic violence, dating violence, and there is more information on that in my written testimony. And we have some of our grantees who are going to be talking here later on the second panel.

I appreciate the opportunity to testify today, and I look forward to continuing to working with Congress, working with you all, as it considers these important issues. Thank you.

[The prepared statement of Ms. Hanson appears as a submission for the record.]

Chairman FRANKEN. Thank you, Ms. Hanson.
Ms. Rich?

STATEMENT OF JESSICA RICH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, D.C.

Ms. RICH. Good afternoon, Chairman Franken and Ranking Member Flake. My name is Jessica Rich, and I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission. I very much appreciate this opportunity to present the Commission's testimony on consumer protection issues involving geolocation information and to offer some initial views on the draft Location Privacy Protection Act.

Protecting consumers' privacy is a key focus of the Commission's efforts, and we commend the Committee for its continued attention to this really important issue.

Products and services that use geolocation data make consumers' lives easier and more efficient, as you have noted, Chairman Franken. Consumers can get turn-by-turn directions to their destinations, find the closest bank, and check the weather when they are traveling, among many other examples.

At the same time, the increasing collection, use, and disclosure of this data presents serious privacy concerns. For this reason, the Commission considers precise geolocation data to be sensitive, warranting opt-in consent prior to collection from a consumer's mobile device.

Why is this data so sensitive? A device's geolocation can reveal consumers' movements in real time and over time and, thus, divulge intimate personal details about them, such as the doctor's office they visit, how often they go, their place of worship, and when and what route their kids walk to school in the morning and return home in the afternoon.

This data can be accessed and used in many ways consumers do not expect, for example, collected through stalking apps, sold to third parties for unspecified uses, paired with other data to build detailed profiles of consumers' activities, or stolen by hackers. The risks to consumer range from unwanted tracking to threats to personal safety.

The Commission has taken action to protect this data through law enforcement and outreach efforts. Using its authority under the FTC Act, the Commission has brought cases against companies engaged in unfair and deceptive practices involving geolocation data. One example is our recent settlement with Snapchat, the developer of a popular mobile messaging app. In that case, the FTC alleged that, in addition to misrepresenting that photo and video messages sent through the service would disappear, which was what was publicized most about that case, Snapchat also collected and transmitted geolocation data from its app, even though its privacy policy claimed it did not track users or access such information at all.

In another case, this one involving the developer of a popular flashlight app, the FTC alleged that the developer told users that it would collect diagnostic and technical information simply to assist with product support, but failed to disclose that the app trans-

mitted the device's precise geolocation and unique device ID to ad networks.

Finally, in a series of settlements with rent-to-own retailer Aaron's and its affiliates, the FTC alleged that the companies' installation and use of software on rental computers that secretly monitored and tracked consumers violated the FTC Act. The software could log keystrokes, capture screen shots, and take photo using the computer's webcam, all unbeknownst to users. Notably, the FTC alleged that installing location-tracking software on the rented computers without the renter's consent and disclosing this geolocation to rent-to-own stores was an unfair and illegal practice.

In addition to enforcement, the Commission also has conducted studies, held workshops, and issued reports in this area. For example, in 2012, FTC staff issued two reports about the disclosures provided in mobile apps for kids. The report showed that the apps collected data from the kids' devices, including unique device ID and geolocation data, and shared it with third parties, often without notice to parents.

And in February of last year, FTC staff issued a report providing specific recommendations about how all players in the mobile ecosystem—platforms, app developers, ad networks, analytics companies, and trade associations—can and must ensure that consumers have timely, easy-to-understand disclosures and choices about what data companies collect and use, including geolocation data.

Now, turning to a discussion of the Location Privacy Protection Act, the Commission very much supports the goals of this bill, which seeks to improve the transparency and consumer control over the collection and use of sensitive geolocation data. The bill really represents an important step forward, notably by requiring clear and accurate disclosures and opt-in consent from consumers before this sensitive data can be collected.

The bill contains both civil and criminal provisions and gives the Department of Justice sole authority to enforce both. We very much support strong remedies for violations. However, as the Federal Government's leading privacy enforcement agency, we do recommend that the Commission be given responsibility for enforcing the civil provisions of the bill.

Thank you very much for this opportunity to provide the Commission's views. The FTC is very committed to protecting the privacy of consumers' geolocation information, and we look forward to continuing to work with the Committee and Congress on this issue.

[The prepared statement of Ms. Rich appears as a submission for the record.]

Chairman FRANKEN. Thank you, Ms. Rich. I noted your recommendation in your written testimony and again just now.

Ms. RICH. Okay. Thanks.

Chairman FRANKEN. Mr. Goldstein?

STATEMENT OF MARK L. GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, D.C.

Mr. GOLDSTEIN. Thank you. Good afternoon, Mr. Chairman, Ranking Member Flake, and members of the Subcommittee. Thank

you for the opportunity to be here this afternoon and provide testimony on consumers' location data.

Smartphones and in-car navigation systems give consumers access to useful location-based services.

However, questions about privacy can arise if companies use or share consumers' location data without their knowledge.

Several agencies have responsibility to address consumers' privacy issues, including the FTC, which has authority to take enforcement actions against unfair or deceptive acts, and the NTIA, which advises the President on telecommunications and information policy issues.

My testimony addresses: one, companies' use and sharing of consumers' location data; two, consumers' location privacy risks; and, three, actions taken by selected companies and Federal agencies to protect consumers' location privacy.

Our findings were as follows in the two reports we released over the last couple of years.

First, that 14 mobile industry companies and 10 in-car navigation providers that GAO examined in its 2012 and 2013 reports, including mobile carriers and auto manufacturers, collect location data and use or share them to provide consumers with location-based services and improve consumer services. For example, mobile carriers and application developers use location data to provide social networking services that are linked to consumers' locations. In-car navigation services use location data to provide services such as turn-by-turn directions and roadside assistance. Location data can also be used and shared to enhance the functionality of services such as search engines to make search results more relevant, for example, returning results of the nearby businesses.

Second, while consumers can benefit from location-based services, their privacy may be at risk when companies collect and share location data. For example, in both our reports, we found that when consumers are unaware that their location data are shared and for what purpose that data might be shared, they may be unable to judge whether location data are shared with trustworthy third parties. Furthermore, when location data are amassed over time, they can create detailed profiles of individual behavior, including habits, preferences, and roads traveled—private information that could be exploited. Additionally, consumers could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods of time or in ways that link the data to individual consumers. Companies can anonymize location data that they use or share in part by removing personally identifying information. However, in our 2013 report, we found that in-car navigation providers that GAO examined used different de-identification methods that may lead to varying levels of protection for consumers.

Third, companies GAO examined in both reports have not consistently implemented practices to protect consumers' location privacy. The companies have taken some steps that align with recommended practices for better protecting consumers' privacy. For example, all the companies we examined in both reports used privacy policies or other disclosures to inform consumers about the collection of location data and other information. However, compa-

nies did not consistently or clearly disclose to consumers what the companies do with these data or third parties with which they might share that data, leaving consumers unable to effectively judge whether such uses of their location data might violate their privacy.

In our 2012 report, we found that Federal agencies have taken steps to address location privacy data through educational outreach events, reports with recommendations to protect consumer privacy, and guidance for industry. For example, the Department of Commerce's NTIA has brought stakeholders together to develop codes of conduct for industry. But GAO found that this effort lacks specific goals, milestones, and performance measures, making it unclear whether the effort would actually even address location privacy. Additionally, in response to a recommendation in GAO's 2012 report, the FTC issued guidance in 2013 to inform companies of the Commission's views on the appropriate actions mobile industry companies should take to disclose their privacy practices and obtain consumers' consent. GAO made recommendations to enhance consumer protections in 2012. GAO recommended, for example, that NTIA develop goals and milestones and measures for its stakeholder initiative. GAO will continue to monitor this effort in the future.

Mr. Chairman, this concludes my oral statement. I would be happy to respond to any comments. Thank you.

[The prepared statement of Mr. Goldstein appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Goldstein. Thank you all for your testimony.

Ms. Hanson and Ms. Rich, your agencies have already done important work to combat cyber stalking and GPS stalking, but I want to challenge you to do more. I want to press you to investigate and shut down these smartphone stalking apps. They hurt tens of thousands of people every year. They market themselves directly and brazenly to stalkers, and they are easily available on the Internet.

My bill will give you even more tools to go after these apps, but will you pledge to me today that you will use all of your existing tools to investigate and shut down these apps?

Ms. RICH. Yes, I will, within my powers. We do have a Commission that needs to approve things, but I run the Bureau of Consumer Protection. I will note that we did bring a case against a similar service called Remote Spy. We litigated a case against them that was providing this very same type of service to spy on people, and we obtained a strong order against the company, and we can use similar tools to pursue these types of stalking apps.

Chairman FRANKEN. Thank you.

Ms. HANSON. From my role at the Office on Violence Against Women, we are a grant-funded organization, and we really want to work with you and work together to address these issues around stalking applications. This has been a huge, a big priority for the Department. I would like to bring back to those folks who actually do the prosecution and want to share your concerns with the Criminal Division, specifically the computer crime and intellectual property section, as well as the U.S. Attorney's Office, Executive

Office of the U.S. Attorney who handles the criminal prosecutions, and I will bring that back to them.

Chairman FRANKEN. Well, thank you. And there is bipartisan agreement on this. In 2011, I sent a letter joined by Senators Grassley, Klobuchar, Cornyn, Blumenthal, Graham, Whitehouse, Schumer, and Feinstein asking your agencies to crack down on these apps. So I want to ask each of you to do everything you can to shut them down.

Mr. Goldstein, some of the witnesses on our second panel urge us to be cautious about legislating. They favor self-regulation. As part of your investigation, you looked at industry best practices for the collection and sharing of location data. In an interview after the report, you said that there were not very many rules in place and that in many ways this was still "the Wild West of the Electronic Era."

Did you find that industry best practices were being implemented consistently? And did you find that consumers were being given the information they needed to make choices about their privacy?

Mr. GOLDSTEIN. Thank you, Mr. Chairman. Our reports clearly indicate that there is no comprehensive approach; that some companies do pay attention very consistently to the rules, the self-regulating rules that are out there, and some do not; and that there is a great variety and not a lot of transparency. Those seem to be the two principal problems, a lot of variety and that some pay attention to some rules and not others, and the lack of transparency and that consumers do not always have enough information to make choices about what kind of information is being retained, how long it is being retained, by whom it is being retained and used, things like that.

So there are quite a lot of problems still out there with the application of the rules.

Chairman FRANKEN. And I see you are nodding, Ms. Rich.

Ms. RICH. Yes. Many industry groups and individual companies say they implement opt-in or have opt-in as a best practice. But our enforcement more broadly, even outside of stalking apps, but related to the collection of geolocation information, including the Snapchat case, the Goldenshores case, which was the flashlight case, our case against Aaron's, and also our survey of kids' apps shows that this opt-in standard is not being complied with on a regular basis.

Chairman FRANKEN. Yes, I found the Snapchat case particularly ironic because their whole selling point was that once you post a video or a photo, it would disappear.

Ms. RICH. And we allege that was not true, among other things.

Chairman FRANKEN. But it did not. Other than that, it was exactly what it said.

Okay. I am running out of my time. I will ask one more question, and we want to get to our other panel, so I will give it to Senator Flake, and I will ask one more question of Ms. Hanson.

Senator FLAKE. Thank you.

Mr. Goldstein, in your testimony you outline a series of "what if's," asserting that location data could be used to track consumers, and I think we all understand the potential of this. You say that

these—which can be used to steal identity, stalk them, monitor them without their knowledge. You also say that collection of data, location data, poses a threat. We all understand that. You have explained that very well. But in your study or in your investigation, did you uncover examples of companies stealing customers' identities or stalking them or criminals' obtaining location data? We know the potential exists. Did you actually turn up any nefarious activity?

Mr. GOLDSTEIN. No, Senator, we did not. It was really a look at the kinds of issues that were out there. It was not really within the scope. But we also did not find any.

Senator FLAKE. Ms. Rich, you mentioned a few of them and cases that have been brought. What has been out there in popular media that has caught your attention? Is that usually how you find these cases? Or how do you come on to these cases where you decide to bring action against them?

Ms. RICH. We find cases in a variety of ways. We may be tipped off by an insider. We may get referrals from businesses or consumer groups or tech people. But responding to the question you just asked my colleague, one thing that our cases do show is that companies, even flashlights, are collecting this data, contrary to the claims they are making, and then they are sharing it. So it is being collected and used, and given what it can show in terms of consumers' private activities, that raises concerns.

Senator FLAKE. Yes, certainly I think we all recognize that people use it for advertising and some of the disclosing—or giving the opportunity to opt out. My question to Mr. Goldstein was do we see criminals using it for purposes that are—the potential certainly exists, but if there are examples of that in a criminal way. We have seen some of the stalking, and obviously we want to make sure that we crack down on that. But I know that the potential exists. I was just wondering, in the studies have we seen that actually occurring? We see some of it on the commercial side, but not so much on the criminal side yet. Is that an accurate statement?

Ms. RICH. I think that the stalking apps are the clearest example of the harm that it can do. I agree.

Senator FLAKE. I mentioned in my opening statement that we want to make sure that we do not stifle any development of new technologies and new positive uses of this geolocation information. Ms. Hanson, the Department of Justice, as you know, works with law enforcement agencies across the country and broadcasters, transportation agencies, and the wireless industry to issue Amber Alerts. The National Center for Missing and Exploited Children manages a secondary distribution of these Amber Alerts. These are obviously only sent when a child is at risk of serious injury or death.

Would Amber Alerts fall within one of the exceptions to the bill?

Ms. HANSON. I would have to bring this back to the Department about how this would be an exception or not. I know that Amber Alerts have been important in identifying missing children. I think we need to look at this issue more broadly, and I can bring that back to the Department to take a look at it.

Through our office, the Office on Violence Against Women, I think, you know, we have seen and you will hear testimony from

folks on the second panel. If you look at the cases of cyber stalking that we actually look at—when you look at it from the perspective of victims of domestic violence, in actuality we do have a large number of victims who have said that they have been tracked. My testimony talked about 72 percent of those reported, looking at victims service agencies, had been tracked by GPS, through cell phone or GPS. So, you know, I think those are important issues we need to look at, but I can bring back this issue, the question about the Amber Alert.

Senator FLAKE. A hypothetical, and some people have talked about and some are actually working on programs, I think, that would send an Amber Alert to a specific location if a child was lost in a mall and you do not need the Amber Alert at that point because there are certain standards and thresholds at which those are issued. But you might be able to send it at a lower threshold if it could be confined to a specific location, say a mall. But obviously, if the geolocation information of individuals who were in that mall, they would not have consented to receive that Amber Alert, they would not have opted in, but could—would this be an exception? And how do we work with the exceptions like that where useful information could go out but not for regulations that could come? Does that make sense? I am sorry.

Ms. HANSON. It makes sense. It is not the area that I work in, so what I would like to do is bring that back to other folks in the Department and get back to you on that.

Senator FLAKE. Okay.

[The information referred to appears as a submission for the record.]

Senator FLAKE. You had a——

Chairman FRANKEN. Well, I just wanted to clarify that an Amber Alert would be—in Section 3 of the bill, we put in exceptions, and any emergency, allowing a parent or legal guardian to locate an emancipated minor child, and also it is for fire, medical, public safety, or other emergency services. So this is specifically in the bill. It would be exempted.

Senator FLAKE. Okay. There are some that are a little less clear. I think Mr. Atkinson in the second panel will note that there are certain programs like Circle of 6, Siren, these apps allow women to share their precise geolocation information with friends who are in an unsafe situation. These, I think we all agree, can be used to help women who are in an unsafe situation. We just want to make sure that we do not do something that would prohibit those kind of uses, and that is a little tougher or a little fuzzier than an Amber Alert. And so I hope as we move through this process—and maybe the second panel can shed some light on that as well.

Thank you, Mr. Chairman.

Chairman FRANKEN. Thank you.

Senator Blumenthal has joined us.

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you to you for having this hearing and for your really instrumental work on a lot of this legislation. Thanks to this excellent panel, and I want to thank particularly Bea Hanson for your work on sexual assault on campuses and your help to me in the roundtables that we organized around Connecticut and the proposals that we formu-

lated as a result, and the President's great work on this issue, thanks to the wonderful staff that he has working on this issue.

To that point, I wonder if you could talk a little bit about what additional steps colleges and universities ought to be taking with respect to cyber stalking and the relationship or the intersection of cyber stalking with campus sexual assault. You know, in Connecticut, more than 50,000 individuals are stalked every year. A lot of it occurs on campuses because college students tend to be more attuned to this technology. And yet I found, as I went around the State of Connecticut, that college administrators and officials there often were not as focused as perhaps they should be on this issue of cyber stalking and the technology that is available to enable it. So perhaps if you could talk a little bit about that issue.

Ms. HANSON. Thank you, Senator Blumenthal. And thank you for your work on addressing campus sexual assault and the report that you put together as a result of all of the hearings you did in Connecticut.

I think that nexus between campus sexual assault and cyber stalking is important, especially when we look at the use of cell phones and smartphones, especially among the college campus students.

There is work that is being done, there is more work that we need to do, in terms of looking at prevention messages and incorporating issues of stalking and cyber stalking, particularly into messages around sexual assault because we know often that stalking is not something that occurs by itself, but that it often escalates over time and can often be a precursor to crimes like sexual assault or even homicide.

I agree with you on your point about the need to train and talk to administrators about it. I think that there is a lot more knowledge among the students than there is among the administrators about the training that is needed to look at cyber stalking and those connections. So we are more than happy to work with you and the rest of the Committee if there are ways that we can make those efforts even stronger.

Senator BLUMENTHAL. I thank you. This technology has huge promise, but also tremendous peril, and the awareness of the peril is sometimes difficult among young people who think of themselves as invincible. And yet because of that delusion, they may be the most vulnerable, and the most vulnerable often to their friends who seemingly want to befriend or support them, and yet use this technology really to put them in great peril. So I thank you for your focus on that.

I would like to ask, Ms. Rich, whether you believe under your current authority you can take action against some of the makers, the manufacturers who may be, knowingly or unknowingly, promoting misuse or abuse of this technology.

Ms. RICH. To date, we have taken action—we did take action and litigated a case against a promoter, a seller of spyware that specifically sold it so that you could capture the movements of somebody secretly. And we did that under our existing authority. We also—I mentioned before you came in, we brought several cases against companies that either under our deception or unfairness authority shared geolocation without consent or notice to consumers. So we

do have authority, but we do need to prove deception or unfairness. And the across-the-board notice and consent requirements with exceptions for legitimate use that are in the proposed—the law which make it easier for us to enforce.

Senator BLUMENTHAL. So you would welcome this additional measure?

Ms. RICH. We very much support the goals and the basic provisions of the bill, yes.

Senator BLUMENTHAL. Do you plan to have roundtables or workshops or other means of increasing awareness among students and others?

Ms. RICH. We recently had a seminar on mall tracking, which is not about stalking but it is about the use of GPS to track consumers' movements in stores, and I think that raised awareness about the use of geolocation, and we will be issuing a report on that. And we will be—we continue to have workshops and seminars on consumer protection issues like these.

Senator BLUMENTHAL. Thank you.

Thank you, Mr. Chairman.

Chairman FRANKEN. Thank you, Senator.

I am going to ask just one real short question of Ms. Hanson, and it is mainly a short answer, I think, that will be required. The latest statistics we have on the prevalence of GPS stalking are from a 2006 study conducted by the Department. Back then, an estimated 25,000 people a year were victims of GPS stalking. That was, again, in 2006, before the explosion of smartphones.

Today the vast majority of adults own a cell phone, and most of them a smartphone. So we just intuitively know that rates of GPS stalking must have increased since then.

Ms. Hanson, my bill will institute regular reporting on GPS stalking, but in the meantime, will DOJ update its statistics on GPS stalking as soon as possible? And if there are barriers in doing that, would you tell me what they are?

Ms. HANSON. Yes, thank you. Thank you for that question. This is a one-time supplement that we had put out in 2006 that was funded by the Office on Violence Against Women. Since then, as I said in my testimony, the National Intimate Partner and Sexual Violence Survey came out in 2011, and the National Institute of Justice as part of the Department of Justice has been working with the CDC on that.

There are questions about stalking, and what I would like to do is go back and talk to folks at BJS and talk to those folks at NISVS to make sure that—to identify if there is any additional stalking questions that would be helpful for us to ask through the Department, just so that we are not duplicating anything that would be in the NISVS report. But I would be happy to go and look into that and get back to you on that, so thank you.

Chairman FRANKEN. Well, thank you very much. I have some questions that I will submit to you for the written record, but I would like to thank all three of you for your testimony and invite up our second panel.

[The questions of Chairman Franken appear as submissions for the record.]

Chairman FRANKEN. All right. I would like to start by introducing our panel.

Detective Brian Hill of Elk River, Minnesota, has served in the Anoka County Sheriff's Office since 2000 and has been a detective with the Criminal Investigation Division since 2008. Detective Hill is an expert in digital forensics and has trained over 3,000 law enforcement officers, prosecutors, judges, advocates, and others across Minnesota on the use of technology to facilitate stalking. He himself was trained by the Minnesota Bureau of Criminal Apprehension, the FBI, and the Secret Service. He also served our country as a member of the Air Force Reserves and was deployed for 2 years for the wars in Iraq and Afghanistan. We are very grateful for your service at home and abroad, Detective Hill, and proud to have you here. Thank you.

Mr. Lou Mastria is the executive director of the Digital Advertising Alliance. He leads the DAA's effort on self-regulation, consumer transparency, and consumer choice. Mr. Mastria is a certified information privacy professional and has served as the chief privacy officer for a range of organizations. Thank you for being here.

Ms. Sally Greenberg is the executive director of the National Consumers League, NCL. She has testified before Congress on a variety of consumer protection issues, including on fraud and excessive fees on car rentals. Previously, she worked at the U.S. Department of Justice and the Anti-Defamation League. Ms. Greenberg was also born and raised in Minnesota and is a graduate of Southwest High School, close to where I grew up in St. Louis Park.

Dr. Robert Atkinson is the founder and president of the Information Technology Innovation Foundation. He holds a Ph.D. in city and regional planning from UNC-Chapel Hill and is a published author on economics and technology policy. Before founding ITIF, he was vice president of the Progressive Policy Institute and director of their new technology project.

Ms. Cindy Southworth is the vice president of development and innovation at the National Network to End Domestic Violence and founder of NNEDV's Safety Net Project. She is one of the Nation's leading experts on stalking apps and has trained thousands of people across the country on stalking apps and the use of technology to facilitate stalking.

Thank you and thanks to all of you again for joining us. Your complete written testimony will be made part of the record. I will note for the record that Ms. Southworth's written testimony on behalf of the National Network to End Domestic Violence is also being submitted on behalf of the Minnesota Coalition for Battered Women.

So why don't we start with Detective Hill. You each have 5 minutes for any opening remarks you would like to make. Detective Hill, please go ahead.

STATEMENT OF BRIAN HILL, DETECTIVE, CRIMINAL INVESTIGATIONS DIVISION, ANOKA COUNTY SHERIFF'S OFFICE, ANDOVER, MINNESOTA

Mr. HILL. Chairman Franken, Ranking Member Flake, and distinguished members of the Subcommittee, my name is Brian Hill,

and I thank you for the opportunity to appear before the Subcommittee to testify about law enforcement's support of the Location Privacy Protection Act of 2014.

Since 2008, I have been a detective with the Criminal Investigations Division of the Anoka County Sheriff's Office in Minnesota. I investigate felony domestic and sexual violence cases with access to Anoka County's state-of-the-art digital forensics lab. I am a computer/mobile device forensic examiner/investigator. The written testimony I submitted details my trainings, certifications, and professional association memberships.

Why is this legislation important? Imagine the trauma of surviving domestic and sexual violence. Now add cyber stalking to that trauma. Stealth stalking apps endanger domestic violence victims' safety, financial stability, and social well-being. As we all increasingly use our cell phones to work, bank, text, access the Internet, e-mail, and pay bills, stalking apps are a tool to isolate victims from the functions and social connections their phones provide, including isolating them from contacting domestic violence advocates or law enforcement.

To be rid of a stealth stalking app, victims must buy new phones, create new e-mail accounts, and change all passwords and security questions. Although there are never any guarantees, victims live with the frightening uncertainty of whether the stealth stalking apps are really gone or if they will reappear after removal. Victims' privacy and peace of mind continue to be violated by this uncertainty, often long after they have bought new phones or changed their passwords.

For instance, I have worked with a victim who suspected that her estranged boyfriend put spyware on her phone. She stated he knew about private phone conversations and text messages. Also, he would show up randomly where she was. I examined her phone and could not get a full data extraction to determine if there was any spyware. Later, she brought in her computer, and I had found her computer has accessed a stalking program called FlexiSPY. There was then proof that the program was installed on her phone. I worked with her on the expensive and complicated tasks of getting a new phone and e-mail account on a safe computer.

Proliferation of cheaper stalking apps has made these harrowing experiences more and more common. In the last 3 years, our mobile forensic exams in our office have increased exponentially by 220 percent in 3 years, averaging 30 exams per month. After 7 years of experience, I continue to discover new apps. For instance, our office is currently investigating an attempted murder in the context of domestic violence. We discovered Ti-spy, running in stealth mode on the victim's mobile device. Ti-Spy advertises itself as a $7 parental monitoring software which can be installed on smartphones to track text messages, calls, GPS location, and basically any phone data.

As in the case of discovering Ti-Spy, I typically become engaged in a forensic investigation after victims or domestic violence advocates detect the unsettling signs of digital wrongdoing. They notice patterns of the abuser's knowledge about the victim's life and whereabouts when the abuser has no way of knowing.

While my department deals with only felony cases, stalking apps are frequently used in misdemeanor domestic violence cases. Investigating cyber stalking is labor intensive and requires expensive, specialized equipment. Most law enforcement agencies, however, do not have the resources, equipment, staffing, or training to examine mobile devices for stalking apps, which can limit data recovery of potential evidence.

Anoka County is fortunate to have eight different tools and dedicated staff for mobile examinations. Because of our county's resources, other counties and Federal agencies request our assistance.

In a survey by the Minnesota Coalition for Battered Women in conjunction with the courts, advocates indicated that cyber stalking was the number one priority for law enforcement training in the protective order context because technology is frequently used to stalk victims and violate protective orders.

To address the need for training on cyber stalking, I have worked closely with the Minnesota Coalition for Battered Women, and its 80-plus member programs, to train over 3,000 domestic and sexual assault advocates, law enforcement, prosecutors, and judges since 2009. Our efforts have borne fruit, but strained resources and the lack of awareness undercut law enforcement's ability to recognize and respond to domestic violence victims' increasing reports of cyber stalking. This erodes victim trust in the criminal justice system. A common abuser tactic in domestic violence is to convince the victim she is crazy. Victims then feel more crazy when they report the abuser has installed stealth stalking apps, only to be told, ″We do not believe you,″ or ″We do not have the resources to examine your phone.″ When law enforcement cannot effectively identify and respond to cyber stalking reports, victims stop reporting crimes and abusers win.

This Act is a major step in addressing the stalking app problem. The most important part is that apps will be required to notify the user a second time, 24 hours to 7 days after initial installation, about the tracking implications. Victims will then be notified when the perpetrator does not have access to their phone. If this notice only applied to stalking apps, they would simply change the name of the app or market it in a different way. Just like in human trafficking, when Craigslist no longer allowed certain ads, the company backpages.com emerged and began to offer those ads. This Act would address such evasion of the law. And it also comes down to economics. By banning stealth GPS stalking apps, we make it unprofitable for the companies to make these programs, which decreases abusers' access to them.

Additionally, the Act brings national public awareness to this issue by requiring information gathering, reporting, and training grants for law enforcement.

Finally, the Act supports victim safety by requiring that all apps get permission to collect or share location information, making sure that a stalking app cannot disguise itself as an employee or family tracking app—or simply as a flashlight app.

I urge you to support the Location Privacy Protection Act of 2014.

Thank you again to the Committee for reviewing my testimony and for your support of law enforcement's efforts to keep domestic violence victims and our communities safe.

[The prepared statement of Mr. Hill appears as a submission for the record.]

Chairman FRANKEN. Thank you, Detective Hill.

Mr. Mastria?

STATEMENT OF LUIGI "LOU" MASTRIA, EXECUTIVE DIRECTOR, DIGITAL ADVERTISING ALLIANCE, WASHINGTON, D.C.

Mr. MASTRIA. Chairman Franken, Ranking Member Flake, members of the Subcommittee, good afternoon and thank you for the opportunity to speak at this important hearing.

My name is Lou Mastria. I am the executive director of the Digital Advertising Alliance, and I am pleased to report to the Committee on how industry has extended its successful online program to mobile to ensure consumers have access to the same transparency control in mobile as they do on desktop.

Of particular interest to this Committee today, our mobile principles require consent for collection of location data and an easy-to-use tool to withdraw such consent, leaving the consumer ultimately in charge.

Last year, the DAA released its Mobile Guidance, providing consumer-friendly privacy controls in this still very fast growing medium. This important, self-initiated update to our principles reflects the market reality that brands and customers increasingly engage with each other on a variety of screens.

The DAA is a cross-industry nonprofit organization founded by the leading advertising and marketing trade associations—the ANA, the 4As, DMA, IAB, AAF, and NAI. These organizations originally came together in 2008 to develop the self-regulatory principles to cover the collection and use of web-viewing data. In 2012, the Obama administration publicly praised the DAA program as a model of success, and more recently, Federal Trade Commission Commissioner Ohlhausen was quoted as calling the DAA "one of the great success stories in the [privacy] space."

The Internet is a tremendous engine of economic growth, supporting the employment of more than 5 million Americans. Mobile advertising by itself in the U.S. totaled more than $7 billion last year, and that is more than a 100-percent increase from the year prior. Revenue from online and mobile advertising subsidizes the content and services we all enjoy.

Research shows that advertisers pay several times more for relevant ads, and as a result, this generates greater revenue to support free content. Consumers also engage more actively with relevant ads. Simply stated, companies have a very vested interest in getting this right.

Self-regulation like the DAA is the ideal way to address the interplay of privacy and online and mobile advertising while preserving innovation. It provides industry, as demonstrated by the multiple updates to our program, with a nimble way of responding to new market challenges presented by a still evolving mobile ecosystem.

The DAA mobile program applies broadly to the diverse set of actors that work together to deliver relevant advertising. The DAA principles call for enhanced notice outside of the privacy policy, consent for location data, and strong, independent enforcement mechanisms.

Together these principles are intended to increase consumers' trust and confidence in how information is gathered in mobile by increasing transparency and control.

The mobile program leverages an already successful universal icon to give consumers transparency and control about data collection and use. In April of this year, DAA issued specific guidance on how to provide this transparency tool in mobile. This will provide companies and consumers a consistent, reliable user experience in the multiple screens on which they interact. This will also provide companies a consumer-friendly way to provide notice and choice outside of the privacy policy. This advancement builds on the unprecedented level of industry cooperation which has led the DAA icon to being served globally more than a trillion times each month.

In the coming months, DAA will also release a new mobile choice app which will empower consumers to make choices about data collected through mobile devices, including applications.

Of particular relevance to this hearing and today, cyber stalking is a serious issue, as was detailed earlier. But criminal activity is separate and apart from the legitimate commercial uses covered by DAA. I want to note DAA's stringent requirements for the collection and use of precise location data for commercial purposes. The DAA program requires consent prior to collection and the provision of an easy-to-use tool to withdraw such consent.

We have required privacy-friendly tools, including notice in the download process, notice at first install, or other similar measures to ensure that companies are transparent in a consistent manner about data collection and that consumers can make informed choices.

To help ensure that both the mechanisms we require are used and that consumer choices are honored, we rely on our accountability programs. Accountability is a key feature of the DAA program. All of our principles are backed by the robust enforcement programs administered by the Better Business Bureau and the Direct Marketing Association. There have been more than three dozen publicly announced enforcement programs under this program to date.

In summary, I would submit that the DAA is a story of empowering consumers through transparency and control. It has nimbly adapted consumer controls to meet quickly evolving market changes and consumer preferences. And it has done so while responsibly supporting the investment necessary to fund free or lower-cost products and services desired by consumers.

I am pleased to answer any questions you might have.

[The prepared statement of Mr. Mastria appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Mastria.

Ms. Greenberg?

STATEMENT OF SALLY GREENBERG, EXECUTIVE DIRECTOR, NATIONAL CONSUMERS LEAGUE, WASHINGTON, D.C.

Ms. GREENBERG. Good afternoon, Chairman Franken, Ranking Member Flake, and members of the subcommittee. My name is Sally Greenberg, and I am the executive director of the National Consumers League. The league was founded in 1899 and is the Nation's pioneering consumer organization. Our nonprofit mission is to advocate on behalf of consumers and workers in the United States and abroad.

Supreme Court Justice Louis Brandeis, who served as NCL's general counsel, noted in a landmark 1928 decision that the right to privacy is "the most comprehensive of rights, and the right most valued by civilized men." We could not agree more. Privacy is a cornerstone of consumer protection and a fundamental human right.

The ubiquity of smartphones, tablets, and other mobile devices has dramatically changed the way consumers interact with the digital world. Thanks to the widespread use of location data, consumers can now navigate to their favorite coffee shops, discover the closest sushi restaurant, and be more easily located by emergency response providers. This technology has clearly provided immense consumer benefits.

However, as the collection and use of location data has become an integral part of the mobile ecosystem, so, too, has consumer concern over the use and misuse of these data. According to a Consumer Reports poll from 2012, 65 percent of consumers were very concerned that smartphone apps could access their personal contacts, photos, location, and other data without their permission.

A similar Los Angeles poll showed that 82 percent of those surveyed were either very or somewhat concerned about the Internet and smartphone firms collecting their information. This should not be surprising. Unlike location data gained from a non-mobile device, such as a desktop computer, data from mobile phones is inherently personal and can be used to learn and possibly disclose information that in many cases consumers would rather be kept private. Justice Sotomayor summed this concern up perfectly in her concurring opinion in *U.S.* v. *Jones*. She noted that, "Disclosed in [GPS] data . . . will be trips . . . to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."

The consensus among consumer privacy advocates and government agencies such as the GAO and FTC that we have just heard from a moment ago is that there is no adequate legal framework protecting consumers' location data in the current and ever-evolving mobile ecosystem. Absent such a framework, consumers must rely on business to adhere to a variety of often voluntary and inconsistently applied company policies and industry best practices. That is why we believe so strongly that this bill is absolutely necessary and will help to protect especially sensitive types of information that consumers use, such as location data.

S. 2171 would do just that. This bill would establish a level playing field for businesses that seek to collect and share location data. It would help to restore consumer trust and location-based services and ensure that the many benefits of this technology continue to

flow to consumers and the economy while adhering to uniform rules of the road for protecting location privacy.

In particular, we believe that the bill's opt-in provisions will allow consumers to take control over their private location information, giving them the right to choose to share that information, or not, and be informed how their location data will be used and by whom. And by prohibiting so-called stalking apps that we have heard so much about, the law will appropriately outlaw a class of inherently deceptive and predatory applications that compromise the personal safety of domestic violence victims. No Federal law currently prohibits the operation of these apps, which are designed to run secretly without the user's knowledge. In addition, we strongly believe that the section providing for private rights of action are critical.

Given the limited resources of Federal enforcement agencies, a narrowly defined private right of action with caps on available damages gives an extra layer of protection to consumers while addressing industry concerns about abuses of that private right of action.

In closing, I would like to reiterate NCL's strong support for S. 2171. In today's ever-changing digital economy, consumers expect and deserve that the privacy of their location information will be protected. Absent such protections, consumers may indeed become less trusting in location-based services, which would be harmful to innovation and the economy as a whole.

Thank you, Mr. Chairman, Mr. Ranking Member, and members of the Subcommittee, on behalf of the National Consumers League and America's consumers, for your leadership in convening this hearing and your invitation to testify on this important issue. I look forward to answering any questions you may have.

[The prepared statement of Ms. Greenberg appears as a submission for the record.]

Chairman FRANKEN. Thank you, Ms. Greenberg.

Dr. Atkinson?

STATEMENT OF ROBERT D. ATKINSON, PH.D., PRESIDENT, THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION, WASHINGTON, D.C.

Mr. ATKINSON. Thank you. My clock is not working, so I will look over here for it. I assume that means I get some time, not zero.

Chairman FRANKEN. I will account for the looking over.

[Laughter.]

Chairman FRANKEN. Ten percent.

Mr. ATKINSON. Thank you. Thank you, Chairman Franken, Ranking Member Flake, and members of the Committee. I appreciate the opportunity to submit testimony today. I am Rob Atkinson, president of the Information Technology and Innovation Foundation, which is a think tank focusing on policies to support technological innovation.

This proposed legislation addresses two very distinct and unrelated issues: One is commercial use of geolocation information by third parties; the second is the use of that information by individuals, particular around stalking. Since these issues are separate and unrelated, I will address them separately.

The issue of limiting the collection of geolocation data by third parties, in our view would stifle innovation in an area that is rapidly evolving. We have seen in the last few years tremendous growth in innovation around location-based services, and, importantly, the U.S. has led in this space. Of the top ten Internet companies in the world, eight of them are American. This is in part because our approach to regulation in this fast-moving digital age has really been to not regulate ahead of time. Unlike Europe, which is home to none of those ten Internet firms, they have embraced the precautionary principle to regulate well in advance of any real harms.

This principle I believe is important for location-based services, especially in part because there is tremendous innovation happening in this space, and innovation that will continue to happen. In fact, we will probably see more innovation in the next 5 years than in the last. Things like in-car navigation and infotainment systems, connected devices making up the Internet of things, facial recognition—these are all interesting and important technologies that, unfortunately, do not lend themselves to a slower-moving regulatory process.

I would support what Mr. Mastria said about industry-led self-regulation being a better approach, at least in this initial stage of technological change and innovation. Clearly, as we heard from Director Rich, the FTC has already taken actions and, in my view, has significant ability to take continued actions.

We already see self-regulation working, for example, the Digital Advertising Initiative, but also on the two major platforms—iOS and Android—consumers have the ability to notice when location is on, to accept it, to not, to turn it off, turn it on.

Second—and I think this is an important point—there is basically at this point no evidence or very little evidence of actual harms arising from commercial use. I will get to the stalking. There are clearly harms there. But in commercial use, I do not believe there is really any evidence of harms. Virtually all of the concern expressed to date by privacy advocates stems from speculative harms that could happen, but not actually ones that have happened.

Third, our view is that some of the provisions in the bill, particularly the private right of action, could be stifling of innovation, particularly in the app space where for the top 800 apps for Android and iOS (Apple), the average company size is 25 employees. A lot of these companies, if they were faced with the potential of a $1 million fine for making a small coding mistake or putting something inaccurate on a website, I believe would think twice about developing a mobile app.

Another component that I think is important is there are many apps that run in the background without the user's knowledge that are actually very, very important. Carrier IQ is an example of that. It is a diagnostic app that many of the mobile carriers use, and it enables the cell system to work effectively so carriers know when calls are dropped, where they are dropped, where they might add cellular capacity. These are apps we want to have running on the phone because they are acting in the public good.

Finally, I would argue that some of the sections dealing with notice can be problematic. For companies to have to list every single company that they deal with from a business perspective could compromise some of their commercial information.

Moving on to the domestic violence issue, I commend you on your efforts there, and I think this is really the most important part of the bill. We certainly fully agree with the outline in Section 4, Criminal Penalties, and Sections 5 through 10. But there are a couple of components that we would want to provide some suggestions on.

The 24-hour to 7-day notice provision as it is written in the bill now, it currently applies to all apps, including applications like, for example, the Weather Channel or Google Maps or Yelp. These are apps where an individual who might put those apps on the phone, they simply cannot get access to the geolocation data. That is third-party geolocation that stays there. That is very different than one of these stalking apps. It is very different than an app like Amber Alert GPS Teen, which is for parents to put something on their kids' cell phone. So I would urge you to think about confining that 24/7 rule only to apps where the individual can get access to the GPS stream and not to have all apps, since the stalker cannot use the Weather Channel, for example, to stalk his or her victim.

I do not think that really mattered, the point that Detective Hill made. The issue here is regulating the behavior of the app. The app could call itself anything, and it would still be under—it would still be subject to this rule if it is allowing the data stream to go to an individual.

Another component I would urge you to think about, and that is international access. One of the concerns we have is even if we can shut down these abysmal stalking apps, stalkers may be able to get access overseas, on overseas websites, and I think thinking about that question, could there be blocking of certain—if we know there is, you know, the same sort of I-Spy site here and it just relocates to the Cayman Islands—could we block access to those?

So, in summary, I will just say that geolocation offers many opportunities for innovation, and regulation at this point is premature. But, again, I commend you, Senator, for your leadership on the criminalization of the stalking apps, in particular, which I think are a serious problem and will help with that.

Thank you.

[The prepared statement of Mr. Atkinson appears as a submission for the record.]

Chairman FRANKEN. Thank you, Dr. Atkinson.

Ms. Southworth?

STATEMENT OF CINDY SOUTHWORTH, VICE PRESIDENT, DEVELOPMENT AND INNOVATION, AND FOUNDER, SAFETY NET TECHNOLOGY PROJECT, NATIONAL NETWORK TO END DOMESTIC VIOLENCE, WASHINGTON, D.C.

Ms. SOUTHWORTH. Good afternoon, Chairman Franken, Ranking Member Flake, and distinguished members of the Committee. My name is Cindy Southworth, and I am the vice president of development and innovation at the National Network to End Domestic Violence. I am also representing our member, the Minnesota Coali-

tion for Battered Women, and I work closely with the Arizona Coalition Against Domestic Violence and the Connecticut Coalition Against Domestic Violence—in fact, all 56 coalitions.

I founded the Safety Net Technology Project in 2002 to support survivors, help victim advocates, train police, and work with technologists and policymakers on thoughtful innovation. We work closely with many technology companies, including Verizon and Google. We serve on the Facebook Safety Advisory Board, and we work with the Application Developers Alliance.

Since 2002, we have presented over 900 trainings to more than 65,000 practitioners. My esteemed and brilliant colleagues are with me today, and I want to say for the record that we love technology. We affectionately think of ourselves as the "geeks of the domestic violence movement."

The previous panel covered the statistics at length, so I will skip that. But I want to say that stalkers use location tracking services, freestanding GPS devices, and smartphone applications.

Phone spyware is one of the most problematic. It allows abusers to monitor much more than location, but location is indeed one of the most dangerous, and it is currently the loophole. This phone spyware does not notify the victim that it has been installed, so an abuser can install it without her knowledge, consent, through any consents, and then it is done.

A standard feature that spy developers go to great lengths to hide is that it is even installed. It does not show up in most phones as an installed app, which seems to be going to great length to hide it. These apps are often brazenly marketed to stalkers, sometimes briefly mentioning employee monitoring and child safety—almost as an afterthought or cover story—and heavily focusing on the features that will help you "spy on your spouse."

One of the most disturbing apps that I have seen recently is called "HelloSpy," and it has a long list of stalking features and has a continuous animated image on their main web page showing a scene from a movie where a man roughly shoves a woman off the bed, backward, head first. It loops over and over and over. And just in the time that I was taking those screen shots, I had to witness that about 100 times to create that poster.

On another HelloSpy web page, there is a photo of a man grabbing a woman's arm, and the woman has visible abrasions on her face. Next to this photo is a list of the features of HelloSpy, including track phone location and many more.

Many of the apps on the next poster that you will see are developed and advertised directly to stalkers to facilitate crimes. In some tragic cases, GPS devices and apps may have actually aided an offender in locating the victim to commit murder. Or in other cases, location tracking was just one piece of an overwhelming list of controlling tactics that preceded a victim's death. For example, in 2009, in Seattle, a man used the location service on his wife's phone to track her to a local store. After finding her speaking to a man there, he shot and killed their five children and then himself.

In Philadelphia, a man installed a tracking device on his ex's new partner's car. Overnight he checked that GPS device 147 times

in one night, hunted him down using the GPS, and stabbed him to death 70 times.

The Electronic Communications Privacy Act, ECPA, prohibits the manufacture, distribution, possession, and advertising of communication intercepting devices; however, it does not cover devices that surreptitiously track location information. Many apps on the poster very likely violate ECPA, and I would be happy to send this poster back with Director Hanson to give to her prosecutor friends at DOJ. It is important to note, however, that there are apps that track only GPS location and do not offer eavesdropping capabilities—and, hence, are not clearly prohibited under Federal law.

Unfortunately, I am aware of only one instance where the Department of Justice has indicted a creator of spyware, and it was the creator of Loverspy, and he promptly fled the country and is now on the FBI's Cyber Most Wanted List. I would be delighted if the developer of HelloSpy would join this creator and be indicted shortly.

So the solution. Number one, we need to require consent prior to tracking or sharing information. Survivors of abuse must be informed about how their location information will be used, disclosed, and shared. This consent process should be prominent, transparent, and easy to understand.

Two, location tracking must be transparent and visible to users. Consent is critical, but consent alone is insufficient. Abusers often install these tracking apps without the knowledge of the victim. Relatively simple safeguards can be added. In fact, some of those safeguards already exist on the Apple technology and even in the Droid technology, letting people know that your location is being tracked.

If GPS technology is being used legitimately to monitor children or employees, there is no need for a stealth mode. In fact, the reputable family safety products are visible.

In 2005, the AntiSpyware Coalition created a consensus definition of spyware, which stated that "tracking software done covertly is spying." And that was developed by technology companies.

This provision, the transparent—the reminder provision is probably the most important element of the bill behind the criminalization. So number three, criminalize the operation, sale, and marketing of technologies whose primary purpose is to surreptitiously track someone's location and facilitate a crime. It is past time to also criminalize intercepting tracking location in addition to intercepting electronic communication.

Four, allow law enforcement to seize the proceeds of those sales. No one should profit from encouraging or enabling criminal acts, and stalking app and device developers are creating and selling crime-facilitating products with abandon.

Five, allow individuals an enforcement option through a very modest private right of action. The proposed protections for victims will be of little use without effective enforcement mechanisms, and the threshold I think is quite low. In fact, our organization has insurance that would cover the accidental oversight, not the punitive but obviously it should not cover that if you are doing it willfully with malintent.

Six, enact parallel State laws. Since the overwhelming majority of stalking and domestic violence investigations are completed at the local level, we are hoping that your bill will become a model for State statutes.

In conclusion, NNEDV supports innovation and has seen countless positive ways that technology can increase the safety and support for survivors of abuse and stalking. We are proud of the close working relationship that we have with technologists, and we thank Verizon, Facebook, Google, Apple, the Application Developers Alliance, and so many more for working with us to increase victim safety. The Location Privacy Protection Act of 2014 will narrowly impact a handful of bad actors that design or operate products created and sold to facilitate terrifying crimes.

Senator Franken, thank you for your tireless and ongoing efforts to end violence against women. Thank you, Ranking Member Flake, and the entire committee for your long support of Violence Against Women Act and these important location protections for survivors.

[The prepared statement of Ms. Southworth appears as a submission for the record.]

Chairman FRANKEN. Thank you, Ms. Southworth. Thank you all.

We are going to have 7-minute rounds for questioning. I will start.

Detective Hill, your testimony mentioned that you are investigating an attempted murder where the victim was being tracked by a stalking app that advertised itself as a parental monitoring software. I actually saw something like that myself. When we had a public hearing to debate this bill 2 years ago, I read from the website of a stalking app named "ePhone Tracker." It looked like this: "Suspect your spouse is cheating? Track every text, every call, and every move they make using our easy cell phone spy software." And there was a lot of press about that after that hearing.

Later the same day, we checked the website again. This is what it looked like: "Is your child exposed to sexting?" And all the stuff about your spouse was gone.

Is it common for stalking apps to disguise themselves like this, Detective Hill?

Mr. HILL. Absolutely. They typically will advertise themselves as being a family tracker or track your employees because they seem more friendly that way.

Chairman FRANKEN. Well, because a lot of people say, well, why don't you just go after stalking apps? Why don't you leave legitimate apps alone? These are really two separate issues. Your answer tells me that if we want to stop stalking apps, we cannot target just apps that label themselves as stalking apps. We also have to lay down a few basic rules of the road for any app that is collecting your basic—your location information.

Mr. HILL. Oh, absolutely, because they will just change the title of their app to something else that stalkers will eventually figure out.

Chairman FRANKEN. Ms. Southworth, we sort of have a needle and thread, I guess. We do not want to interfere with the legitimate parental monitoring apps, but we do want to block stalking

apps that are pretending to be something that they are not. How do you do that?

Ms. SOUTHWORTH. Legitimate parental monitoring apps, if they follow along with the best practice of the computer-based monitoring apps, are visible. With the Microsoft Family Safety product, the child knows they are being monitored and their parents have control functions. From the moment they turn the computer on, they can see that there is monitoring occurring. The same with employee monitoring products. There is absolutely no problem with knowing that your device or your computer is being monitored. So it is—in fact, the spyware industry definition says if it is a monitoring product, it is spying if is not visible to the user, and there is no exception for child or employee. I understand that a child would not need to consent in the U.S. under our law, but they would still need notice.

Chairman FRANKEN. Well, thank you, and I agree with you that the reminder provision is absolutely critical here. Dr. Atkinson has actually raised a couple of concerns about the reminder provision, so I want to turn to those. Dr. Atkinson, in your testimony, you say that reminders might make it harder for parents to keep track of their kids because the kids will know they are being tracked. As you just heard, though, we cannot limit reminders only to apps that call themselves stalking apps. A lot of stalking apps pretend to be parental tracking apps and things like that.

More importantly, though, I disagree with you that the reminder provision "would be applied too broadly to all apps using geolocation data," from your testimony. My bill requires reminders only if an app is running in a way that is imperceptible. I am not sure—you seem to miss that because in your testimony you cite the Passbook app, in your written testimony, for the iPhone as a legitimate app that "is arguably 'imperceptible to the user.'"

Well, I took a look at my home screen on my iPhone, and there it was. This was not my iPhone, but it is second from the left on the top there, and it shows up on your home screen by default. In fact, you cannot delete it. It is impossible to delete, and every time it gets your location, a little arrow pops up. Show the arrow next to the 92 percent. I do not know if you can see this. It is also in your privacy settings under location services.

So the Passbook app that your testimony says is imperceptible is really easy to perceive, at least to me. Any app like the Passbook app would not have to remind their users of anything under my bill. My point, though, is that it is not a fluke that Passbook app is running transparently. That is just the industry best practice. So right there, any app that follows best practices will not have to send any extra reminders.

So, Dr. Atkinson, isn't it already industry best practice that location apps run in a way that are transparent to the user?

Mr. ATKINSON. So my point with that was twofold. One was—and I may have made—should have made that clear. "Imperceptible" is perhaps a vague standard and perhaps you might look at what would be a better definition in the bill of what is actually imperceptible. Is imperceptible related to the size of the icon? Is it related to being able to see in the list? That was one point I was trying to make there.

I fully agree with you that—there are tracking apps, if you will, are apps that report location that do run in the background, like Carrier IQ. And those are used—those, again, are not applications that an individual can access. I cannot go to the Carrier IQ website and find out where my phone was. So that was really the point I was making, is make sure that—I would encourage you to make sure that the definition of any of these applications is only for those apps where an individual could put something on the phone and then the individual could get access to that geo data stream. Otherwise, there are other apps that are sometimes used for system performance where you would not want that to be the case.

Chairman FRANKEN. Well, I really do not think Carrier IQ should be a model here. In 2011, in fact, we had—people were outraged when they found out that the software was running in secret, and so outraged that Sprint, the single biggest user of Carrier IQ, removed the software from tens of millions—26 million devices. And I am sure that there are isolated cases where the reminder provision might be superfluous and where it might be difficult. But, I mean, imperceivable, when it is on the home page, is—I do not know exactly—this just seems very—by and large, very straightforward to me.

But I have run out of time, and I will go to the Ranking Member.

Senator FLAKE. Well, thank you.

Mr. Atkinson, in your testimony, you note in the written testimony there are number of innovative new products that would be considered mobile devices under the legislation, but they are not smartphones. These are like smart shoe apps or watches or other help devices that use location data to tell you how many steps you have walked that day. But these do not allow notification. There is no interaction with the user. Would that stifle innovation in these areas if you have issues or regulations that cover that?

Mr. ATKINSON. I think it could. Ms. Southworth mentioned an app which is just simply a GPS device. And, in fact, the company I mentioned, the Amber Alert company, they actually sell just a pure GPS device you could put in your child's backpack so you can follow them around and make sure you know where they are.

There is no real way to do notification on that device, so a stalker, for example, could, as she said, put one of those devices in someone's trunk of their car. While I support the notion that we should have notice on those for stalking apps, there are certainly other technologies where you could not do that. And then obviously on some of the new things that we are going to get, how would you do a notice, for example, on a shoe or a shirt or other things like that? It could be hard to do notice. Notice is easier when you are dealing with an actual computer-like device.

Senator FLAKE. Right. Mr. Atkinson, following up on that, Ms. Southworth at the end of her testimony said that the Location Privacy Protection Act will "narrowly impact a handful of bad actors that design or operate products created and sold to facilitate terrifying crimes." Is that an accurate description of the legislation, that it would simply impact a handful of bad actors?

Mr. ATKINSON. Certainly the component—some of the components, particularly toward the end of the bill, would certainly do that and are needed. But half of the bill or some share like that

is really focused on just broad generalized commercial use of geolocation data, which has, frankly, nothing to do with stalking, has no relationship to stalking or identity theft or other problems. And the bill would address those issues, and I think in a way that perhaps could limit innovation.

Senator FLAKE. I certainly agree on the point, and like I said, there is a big part of the bill that I support, the stalking legislation part of it. But I remain concerned about some of it stifling innovation you were talking about.

Mr. Mastria, do you want to address that as well?

Mr. MASTRIA. Senator Flake, thank you. We see that self-regulation has been both effective and up to the task to give consumers transparency and control around the—certainly on the desktop environment, and will bring that to the mobile environment. The desktop environment we have been in for over 3 years. Later on this year we will be releasing our mobile choice app, which has been a work in progress now for about a year. We released our Mobile Guidance last year. We released an industry code for how to display notice earlier this year. The mobile app will be the third step in a four-step process that will actually make the guidance enforceable.

Senator FLAKE. Do you share Mr. Atkinson's concerns that some of these new devices are not interactive and there is no way for even best practices or businesses to band together for notification if there is no interaction with the user? Does that, in your view, stifle innovation?

Mr. MASTRIA. So one of the reasons that we think that self-regulation works—and I just want to limit my answer to the scope of the program that I run. One of the reasons that we think that innovation is better served by self-regulation is that we can quickly adapt and quickly move to new business models. Not that many folks were simply thinking about apps and cross-app data, precise location data many years ago, but we have not only a set of principles in place and guidance for companies to follow, but we are also putting out tools for consumers to be able to make choices.

So that has happened in a fairly quick amount of time. I think if there are challenges in the future around that, self-regulation seems to be a quick way to adapt to those changes.

Senator FLAKE. In your view that could be far more nimble than perhaps Government regulation in this regard?

Mr. MASTRIA. I think that is more eloquently put than I did. Yes, thank you.

Senator FLAKE. Ms. Greenberg, you state in your testimony, "... if companies affirmatively state in their privacy policies that they will collect and share their users' location data without consent with any third party they wish, they are free to do so and the FTC has little power to stop them." But in that scenario, doesn't the consumer have the ability not to use the company's service or the app?

Ms. GREENBERG. Well, certainly that is true, but there are many, many apps that consumers find very useful. I do not think that should mean that they sacrifice their privacy or their ability to say, "What are you using this data for? Don't I have the right to say you need to let me know that this information is being shared and

with whom it is being shared?" So I think we can bridge that gap without interfering with companies' ability to innovate.

Senator FLAKE. Mr. Atkinson, again, you noted in your testimony there were many beneficial uses of tracking apps. You mentioned examples of the loved one locator, Project Life Saver; if someone has autism or dementia or Alzheimer's, family members are able to track and make sure that there is a safe zone that they stay within.

There are exceptions in the bill, exemptions in the bill for that, but some concerns have been raised where there are situations where a sibling or a close family friend or others who are not a parent or legal guardian might want to be involved in that. Do you want to address that again or in more detail?

Mr. ATKINSON. Sure. I think it is important to understand that "stalking" is not a technological term. It is a behavioral term. "Tracking" is the technological term. And I do not believe—nor does the bill do this—that we should ban tracking applications. There are enormous benefits for families, for other people to want to know where their device is, where their family members are. And we need to make sure that we can go forward with those.

What I am somewhat concerned about—I do not believe we will end up with a situation where we can—I think companies will change their names. They will just be Family Trackers, or stalkers will just use Family Trackers. But fundamentally I do not know how we can solve the problem, because, for example, on the notification, any person who installs an app on a phone, on the iOS or Android, you can turn off notification.

Now, you can hope that the person whose phone it is understands that and looks at it, and I think that would be part of the education effort we need to do. But how do you monitor your phone? How do you look at the apps running list, all those things? But there is simply—in both of those operating systems right now you can just say, "Turn off notification."

So I think it is a little more complicated, I think, than just simply taking a set of apps that are bad actors who have used them for bad purposes.

Senator FLAKE. Thank you.

Thank you, Mr. Chairman.

Chairman FRANKEN. Thank you. The emergency exception and public safety exception are not limited to parents. I just wanted you to know that.

Let us talk about a couple things. Mr. Mastria, both you and Dr. Atkinson have referred to Digital Advertising Alliance's self-regulatory program for mobile marketing as a model program. But just so I am clear, you issued this code in July 2013, but you are not enforcing it. Is that correct?

Mr. MASTRIA. The code was issued in July 2013. There had to be several operational steps that have to be put into place before it can become operational. One of them is that there had to be a standardized way for companies to display the notice to consumers. That happened in April. And the next step is to have an app so that consumers can express their choices. The next step after the app would be that enforcement would come. Once a consumer

makes a choice, we want to make sure that that choice is honored and that companies are held to honoring that choice.

Chairman FRANKEN. So it is a model program in theory.

Mr. MASTRIA. No. The desktop program version of this has been around for almost 3½ years.

Chairman FRANKEN. Okay.

Mr. MASTRIA. So we have a great pedigree to show that, in fact, we do put the tools in market that we say we will.

Chairman FRANKEN. Okay. Well, can I ask, Ms. Greenberg, about what your opinion is of—you know, what the reality you see is in best practices?

Ms. GREENBERG. Well, it seems that DAA's code is coming late in the game—other industry players like CTIA and the Direct Marketing Association put codes in place years ago. And so with all due respect to Mr. Mastria—and we have looked at his code, it is full of holes. We would argue that it feels like a PR gesture and may be driven, in fact, by the introduction of this legislation.

And I would also take issue with the idea that self-regulation is working. There is monumental evidence that self-regulation is not working. We have heard witnesses from GAO and the FTC say as much. The Wall Street Journal did an article that you mentioned with 101 apps being tested, and 47 of those disclosed users' location to a third party without user consent.

So I would say we very much need this bill because self-regulation is not protecting consumers.

Chairman FRANKEN. You know, there is the point that the Ranking Member made: Has there been any evidence of harm? I think that most Americans believe in that they have some right to privacy. Do you think that there is harm that individuals can feel if their privacy is not being protected?

Ms. GREENBERG. Yes, the notion that there is no real harm from the tracking and using of location data for consumers really strikes at the heart of our notions of consumer protection and the idea that privacy is a bedrock American principle. We know that Justices of the Supreme Court whom I mentioned, Brandeis and Sotomayor, have articulated that that is a bedrock right. And we see from the Consumer Reports surveys, from the L.A. Times survey, the vast majority of consumers do care about their location data not being shared without their consent and do want to know where that location data is being sent and that it is being shared and for what purpose.

So I think that flies in the face of what we know about how consumers feel about their privacy.

Chairman FRANKEN. Dr. Atkinson, last year your organization published a blog post about my location bill, and in it said that, "The evidence for the use of stalking apps by stalkers and harassers is somewhat thin."

Dr. Atkinson, I can understand how an economics think tank might think that, but I am curious what folks in the field have actually seen.

Detective Hill, are stalking apps common or is the evidence of their prevalence somewhat thin?

Mr. HILL. They are very common, and the more exams we have done—like I said, you know, our exams have increased 220 percent.

The more exams we do, we are finding more and more that these apps do exist and are on phones.

Chairman FRANKEN. Ms. Southworth?

Ms. SOUTHWORTH. A week does not go by where our national office—we are not even set up to do direct services, but we get calls every single week from survivors who are really trying to figure out is the GPS device on my car, is it on the phone, is it an app, is it a setting. And we have a lot of work to do to help them try to figure it out, and we just do not have enough Detective Hills out there to send them to have those phones examined.

Chairman FRANKEN. Right, and that is why we are hoping—and I think Dr. Atkinson has stated his general approval of the stalking apps piece of this, so I do not want to send that wrong message. Just in the execution of it, in terms of giving—how important is it—and I will go to you again, Ms. Southworth—that people have a reminder that this is happening? And how realistic is that? Because Dr. Atkinson talked about your being able to suppress that.

Ms. SOUTHWORTH. It is vital, and the behavior is not new. As all the witnesses have said, you know, there is general support around helping victims. The challenge is offenders will do anything they can to control and monitor their victims, and back in the day they would look at the odometer when a victim went to the grocery store and see if she perhaps stopped to pick up a prescription because that is outside of the bounds of what she was allowed to do that day, that just phenomenal, crazy, and out of control that offenders do.

What happens with some offenders is they will actually tell the victim, "I am putting this stalking app on your phone, and I am going to be tracking you." If she knows it is there, when she comes to meet with Detective Hill to file a report, or she goes to the local advocate to meet and talk about a protection order, she can accidentally let the battery run dead. She can leave the phone behind. But if she does not know it is on the phone because either the offender did not tell her or she does not see it, there is no little arrow on the top, she cannot do anything to stay safe.

Chairman FRANKEN. Before I run out of time, I mean, this goes to the resources, because someone who feels like they are being tracked, saying it must be in this thing, what happens when they go to a police station routinely?

Mr. HILL. Routinely what happens is the agencies do not have the tools to look at it, so they say they cannot, or they may only have one tool to look at it, and they quick take a look at it and do not see anything, and then send the victim on their way, which can be very frustrating.

Chairman FRANKEN. This is why we need and the bill does get resources for being able to do exactly what victims need.

Mr. HILL. Absolutely.

Chairman FRANKEN. Okay. I am out of time, and we will go back to the Ranking Member, if you have any more questions.

Senator FLAKE. Well, I appreciate that. Let me just say, like I said, the portions of the bill that deal with stalking, I applaud the Chairman for his dedication on this, and those who have testified, and groups and organizations that have worked on this for a long time. And I do think we definitely need action in those areas. My

concern is just we in other areas, the other part of the bill, that we do not unnecessary stifle innovation that could help with some of these same areas we are talking about.

But, Mr. Mastria, I think concerns have been raised about this legislation, that it might require notice to be provided and consent be obtained for individuals using a device. But some devices are used not just by one individual, a family table or a GPS in a car. Is there a concern among some members in your organization that notification may be given to an individual but not others who use the same device? Is that a concern?

Mr. MASTRIA. Senator, I can speak to what the program code is, and the program says that if you are transferring location information, you have to get consent, and you have to get it either at the download or on install, at some point that is obvious. It has to be clear, meaningful, and prominent.

I would like to take a step back and just answer a point that Ms. Greenberg made. Thank you for mentioning CTIA and DMA. They were both participants in the development of our code, and our code will be enforceable later on this year.

In terms of the PR piece, our program has announced more than 30 public actions against both participants of the DAA and nonparticipants alike. That is not PR. It is not an easy conversation to have with a company that they are somehow noncompliant with our program. But the reality is that that is the mission that we have set out to do. The FTC had asked us to mount a program, challenged industry to mount a program to deliver transparency, control, and accountability, and we do that every single day. And that is the program that we have, and we think that it serves both industry and consumers well.

Senator FLAKE. Thank you. That was my next question, actually, to describe the program you have with companies to, you know, give some discipline to what you are talking about. And you have actually referred companies for investigation. How many did you say?

Mr. MASTRIA. There have been 33 public compliance actions. That number, I think it is in the 60 or 70 individual companies that are named in there, and of those, we get compliance from most of them eventually. But one of them did get referred to a Federal authority.

Senator FLAKE. Well, thank you. That does it for me, and I really appreciate this hearing, and thank you for your testimony, everyone.

Thank you, Mr. Chairman.

Chairman FRANKEN. Well, I would like to thank all the witnesses. Very, very quickly, because I do not want to have a long back-and-forth, but would you like to respond to that, Ms. Greenberg. But, again——

Ms. GREENBERG. Yes, if I could just take a——

Chairman FRANKEN. If you take a lot of time, I am going to go back to Mr. Mastria.

Ms. GREENBERG. I will just take a moment to say it is not that we are arguing with the idea that they may have pursued investigations. It is the code itself that is weak. The way we read the code, an app does not need to get permission if they do not share

the data and they keep it to themselves under the code. And if the app does share precise location with a totally different company, they still do not need to get permission to share it if they are doing so for a variety of purposes, like market research or product hits.

So, in other words, it is the code itself that is weak, and when I described it as full of holes, that is what I was referring to.

Chairman FRANKEN. I will go back to Mr. Mastria, just in fairness.

Mr. MASTRIA. The code does call for consent when there is a transfer of location information, and the reason we do that is that we focus on when information is being transferred to unrelated apps or unrelated sites. And so that is the code, and that is part of the transparent——

Chairman FRANKEN. Well, was her characterization of the code not accurate?

Mr. MASTRIA. Yes; not accurate. I think that we focus on transfer of information to unrelated apps, unrelated sites, and we want to make consumers aware of that. We want to give them control over that. That is the part of the code that is really kind of the most—the essential piece of the DAA program.

Chairman FRANKEN. Okay. We may follow up.

Mr. MASTRIA. Yes.

Chairman FRANKEN. I do not want to—okay. I do not want to do whatever I would be doing if I did it.

So, in closing, I want to thank obviously the Ranking Member, Senator Flake, thank you, and I want to thank each of the witnesses, and every one of you who appeared today, and particular Detective Hill, who took time out of his job to travel here and to testify to us. We heard a lot of valuable testimony today. I think that my bill is going to protect our privacy without—I think it would not create difficulties for industry, and I am going to think about today's testimony, though, and other feedback that we get, and we will work to address that feedback to make any needed improvements in the bill between now and the time it gets a vote.

So I thank all of you, and I mean that sincerely, I thank all of you for being here. But I think there is one thing that there is absolutely no question about. Stalking apps must be shut down. It is unacceptable that in this day and age companies are making money off of stalking and brazenly marketing themselves to stalkers. It is equally unacceptable that our laws have loopholes that let them do this. No matter what we do, no matter what form this bill takes, we have to stop these apps. I think there is agreement here.

So we will hold the record open for 1 week for submission of questions for the witnesses and other materials. Thank you, thank you, thank you again. This hearing is adjourned.

[Whereupon, at 4:32 p.m., the Subcommittee was adjourned.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

UPDATED Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

On

"The Location Privacy Protection Act of 2014"

Wednesday, June 4, 2014
Dirksen Senate Office Building, Room 226
2:30 p.m.

Panel I

Bea Hanson
Principal Deputy Director
Office on Violence Against Women
Department of Justice
Washington, DC

Jessica Rich
Director
Bureau of Consumer Protection
Federal Trade Commission
Washington, DC

Mark Goldstein
Director
Physical Infrastructure Issues
U.S. Government Accountability Office
Washington, DC

Panel II

Detective Brian Hill
Anoka County Sheriff's Office
Criminal Investigation Division
Andover, MN

Lou Mastria
Executive Director
Digital Advertising Association
Washington, DC

Sally Greenberg
Executive Director
National Consumers League
Washington, DC

Dr. Robert D. Atkinson
President
Information Technology and Innovation Foundation
Washington, DC

Cindy Southworth
Vice President
Development and Innovation
National Network to End Domestic Violence
Washington, DC

PREPARED STATEMENT OF BEA HANSON

Department of Justice

STATEMENT OF

BEA HANSON
PRINCIPAL DEPUTY DIRECTOR
OFFICE ON VIOLENCE AGAINST WOMEN

BEFORE THE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW
UNITED STATES SENATE

AT A HEARING ENTITLED

"THE LOCATION PRIVACY PROTECTION ACT OF 2014"

PRESENTED
JUNE 4, 2014

Testimony of Bea Hanson, Principal Deputy Director
Office on Violence Against Women

Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

"The Location Privacy Protection Act of 2014"
June 4, 2014

Introduction

Good afternoon, Chairman Franken, Ranking Member Grassley, and Members of the Committee. Thank you for this opportunity to testify on behalf of the Department of Justice regarding stalking, mobile devices, and location privacy.

My name is Bea Hanson, and I am the Principal Deputy Director of the United States Department of Justice Office on Violence Against Women (OVW). The Department of Justice has focused on strengthening the criminal justice response to stalking through its implementation of the Violence Against Women Act (VAWA). Since the passage of VAWA in 1994, we have made significant strides in enhancing the criminal justice system's response to stalking. Today, stalking is a crime under the Uniform Code of Military Justice, the laws of the District of Columbia, all 50 states, and under federal law, which extends to the U.S. territories and Indian country. In 2005, the federal interstate stalking statute was broadened to protect victims of cyberstalking and enhance penalties for repeat stalking offenders. In addition, the recent reauthorization of VAWA amended the Jeanne Clery Act to mandate that colleges report crime statistics on incidents of stalking.

Stalking is a complex crime that is often missed, misunderstood, and underestimated. . Stalking is a course of conduct directed at a specific person that causes the targeted individual to fear for their safety or the safety of their family members. Victims feel isolated, vulnerable, and frightened, tend to suffer from anxiety, depression, and insomnia, and lose time from work as a result. Many victims have no choice but to move or change jobs due to their victimization.

Incidents of stalking behavior, when considered separately, may seem relatively innocuous. Stalking tends to escalate over time, and is often paired with or followed by sexual assault, physical abuse, or homicide

Results of the 2010 National Intimate Partner and Sexual Violence Survey (NISVS), released by the Centers for Disease Control (CDC) in late 2011, demonstrate the degree to which stalking threatens the well-being and safety of individuals across the

United States. Using a conservative definition of stalking, which required respondents to report stalking in which they felt very fearful or believed that they or someone close to them would be killed or harmed, the survey found that 6.6 million people were stalked in a 12-month period and that 1 in 6 women and 1 in 19 men were stalked at some point in their lifetime.[1]

The report noted that, although anyone can be a victim of stalking, females were more than three times more likely to be stalked than males,[2] and that young adults had the highest rates of stalking victimization. More than one-half of female victims and one-third of male victims were stalked before the age of 25. In addition, about 1 in 5 female victims and 1 in 14 male victims experienced stalking between the ages of 11 and 17.[3]

The NISVS also revealed the too frequent nexus between stalking and intimate partner abuse. For the overwhelming majority of victims, the stalker is someone known to them – an acquaintance, a family member, or, most often, a current or former intimate partner. Sixty-six percent of female victims and 41 percent of male victims were stalked by a current or former intimate partner.[4] Statistics provided to the Office on Violence Against Women by our own grantees tell a similar story: in one recent reporting period, our discretionary grantees reported that 70 percent of the stalking victims that they served had been victimized by a current or former spouse or intimate partner or dating partner; subgrantees of our STOP Violence Against Women Formula Program reported the same for 61 percent of the stalking victims they served.[5]

And, the NISVS report confirmed what law enforcement, prosecutors, victim service providers, and other professionals have been hearing from victims for years—that most stalking cases involve some form of technology. More than three-quarters of victims reported having received unwanted phone calls, voice and text messages; and roughly one-third of victims were watched, followed, or tracked with a listening or other device.[6] Indeed, the NISVS authors noted that their findings show a higher percentage of stalking than previous national studies and hypothesized that this higher rate could be due to the growth of new technologies that did not exist as stalking modalities when some earlier studies were conducted. As the NISVS authors recognized, the recent tremendous

---

[1] Black, M.C., Basile, K.C., Breiding, M.J., Smith, S.G., Walters, M.L., Merrick, M.T., Chen, J., & Stevens, M.R. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, p 29-31. NISVS also reported stalking prevalence using a less conservative definition of stalking, which considers any amount of fear (i.e., a little fearful, somewhat fearful, or very fearful). Using that definition, the study found that 1 in 4 women and 1 in 13 men reported being a victim of stalking in their lifetime, with 6.5% and 2.0% of women and men, respectively, reporting stalking in the 12 months prior to taking the survey. *Id.* at 29.

[2] *Id.* at 30.

[3] *Id.* at 34.

[4] *Id.* at 32.

[5] Data on file with Office on Violence Against Women.

[6] NISVS Summary Report at 31.

growth in cellphone ownership and wireless technology may have increased the ease with which offenders engage in stalking behaviors.[7]

These findings underscore how critical it is that professionals who respond to and work with stalking victims understand the dynamics of stalking, particularly how stalkers use technology. At OVW, we know that stalking is often a precursor to other forms of violence, including rape, sexual assault, physical assault, and homicide. Because stalking can be challenging to recognize, OVW grant programs support specialized training for law enforcement, prosecutors, parole and probation officers, and victim service providers to recognize stalking, to aggressively investigate and prosecute cases, and to ensure that comprehensive, holistic services are available for victims.

Cyberstalking

The spread of cellular phones in recent years has created a new market in malicious software that, when installed on mobile devices, allows perpetrators to intercept victims' communications without their knowledge or consent. Through the use of this software, perpetrators can read victims' email and text messages, listen to victims' telephone calls, trace victims' movements, and turn on the microphone in victims' phone to record conversations occurring in the area nearby. All of this can be done remotely and surreptitiously. This conduct has far-reaching security implications. This spyware can be used by competitors to commit corporate espionage, by abusers to stalk their former partners, and even as part of an effort to spy on law enforcement and national security personnel. One important consequence of the proliferation of spyware that collects communications and location information is the risk that stalkers, abusers, and others intent on victimizing the user could use information collected on their mobile devices.

Technology is often a tool of abuse in teen relationships.[8] Research shows that young women ages 18-24 experience the highest rate of stalking[9] and that over a quarter of stalking victims report being stalked through the internet or electronic monitoring.[10] Stalkers will sometimes make hundreds of unwanted phone calls, while also sending text messages, instant messages, or emails to the victim. This harassing contact is common in teen dating violence.[11] One in four teens in a relationship has been called names, harassed, or put down by their partner through cell phones and texting.[12]

---

[7] *Id.* at 84.

[8] Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010). The new age of stalking: Technological implications for stalking. *Juvenile and Family Court Journal, 61*(4), 39-55.

[9] Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking victimization in the United States. Bureau of Justice Statistics Special Report* (No. NCJRS 224527). Washington, DC: U.S. Department of Justice. Catalano, S. (2012) *Stalking victims in the United States – revised.* Bureau of Justice Statistics Special Report. Washington, DC: U.S. Department of Justice.

[10] Baum, Catalano, Rand, & Rose, 2009

[11] Fraser, Olsen, Lee, Southworth, & Tucker, 2010.

[12] Lenhart, A., Ling, R., Campbell, S., And Purcell, K. (2010). Teens and Mobile Phones. Pew Internet and American Life Project.

OVW funds a number of projects that target the intersection of technology and the crimes of stalking, sexual assault, domestic violence, and dating violence. We recognize that stalkers are increasingly abusing a variety of telephone, surveillance, and computer technologies to harass, terrify, intimidate, and monitor their victims, including former and current intimate partners. For young victims in particular, new technologies bring the risk of digital abuses such as unwanted and repeated texts, breaking into personal email accounts, and pressure for private pictures. Three OVW-funded projects, in particular, focus on "high-tech" stalking and the dangers that new technologies pose for victims.

First, for over thirteen years, OVW has funded the Stalking Resource Center, a program of the National Center for Victims of Crime, to provide training and technical assistance to our grantees and others on developing an effective response to the crime of stalking. The Stalking Resource Center has trained and provided technical assistance to over 100,000 multi-disciplinary professionals nationwide, with an emphasis on the use of technology to stalk. Among other projects, the Resource Center has co-hosted eleven national conferences that specifically focused on the use of technology in intimate partner stalking cases. In addition, with funding from the Department's Office for Victims of Crime, the Stalking Resource Center developed two training tools focused specifically on the use of technology to stalk. The first is a 15-minute training DVD and discussion guide designed to help law enforcement officers, victim advocates, and allied professionals understand the most common forms of technology used by stalkers. The second is a self-paced, interactive online training course that explores many of the technologies used by stalkers and discusses how to document and obtain evidence related to these technologies as well as considerations for victim safety.

Second, since 2004, the National Network to End Domestic Violence's (NNEDV) Safety Net project has been funded by OVW to provide unique technical assistance and training to a wide range of grantees to address how technology issues impact the safety, privacy and accessibility rights of victims of domestic violence, dating violence, sexual assault and stalking. The project also educates grantees on ways to use technology strategically to help victims find safety and increase program efficiency, and trains law enforcement officers and justice system officials, social services providers, coordinated community response teams, and others about how to hold perpetrators accountable for misusing technology against victims of abuse and stalking. As an OVW technical assistance provider on technology safety, NNEDV trained – in just the past two years – more than 3,000 advocates, attorneys, court personnel, service providers and other professionals. In that same time period, NNEDV responded to 783 requests for in-depth and nuanced technical assistance, often spending days researching and assisting just one grantee. To serve survivors of violence and abuse, OVW partnered with NNEDV to develop the Technology and Confidentiality Online Toolkit (http://tools.nnedv.org), a website that provides updated information and resources for agencies, co-located partnerships (serving victims of domestic violence and sexual assault), and coordinated community response teams receive the coordinated services they need while maintaining the victims' privacy, confidentiality and ownership over their personal identifying information.

Third, OVW funds the Family Violence Prevention Fund's "That's Not Cool" campaign to assist teens in understanding, recognizing and responding to teen dating violence. A critical part of this project addresses cyberstalking by helping teens define their "digital line" as it relates to relationship and dating abuse. The website www.thatsnotcool.com was launched in January 2009 to help teens identify digital dating abuse and to encourage them to define for themselves what is and is not appropriate. So far the campaign has produced strong results in raising awareness of the issue and available resources, including over 3 million website visits and 77,000 Facebook fans.

VAWA-funded Support for State Prosecutions

VAWA grant programs promote effective strategies to address stalking cases which present many challenges for law enforcement and prosecutors. VAWA funding supports the development of investigative and prosecution policies and procedures for stalking cases, training on stalking, increased staffing, establishment or expansion of specialized stalking units, upgrades to databases and technical assistance on complex cases. A state prosecutor with funding from the Grants to Encourage Arrest Policies and Enforcement of Protection Orders Program reports that:

> I have been working with a victim since July of 2012 on a stalking case. The suspect was arrested in 2011 for burglary and assault, and a no contact order was put in place. The victim came to me directly as she didn't feel anyone else would believe her. The suspect is a doctor in town, and he had manipulated her for years. She showed me a box of evidence which contained emails and texts from this anonymous person, who had been harassing her for months. The texts were extremely personal and derogatory. Some of the texts recommended the victim get back together with the suspect. When I read the texts, I felt strongly that it was the same suspect who had assaulted her. I started sending out subpoenas to gain Internet Provider address information on these contacts. I was able to confirm it was indeed the same suspect who assaulted her back in 2011. [The suspect] was arrested . . . and [s]ince that time, I confirmed that 3 different types of contact (hundreds of texts and emails) all come back to that same suspect, making this a very strong case.

Federal Prosecutions

Although most stalking offenses are best handled by state and local police departments and prosecutors, the Department has also responded to the cyberstalking challenge through the prosecution of violations of the federal cyberstalking prohibition, 18 U.S.C. § 2261A(2). This statute allows for the prosecution of individuals who stalk using "the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce...." This prohibition encompasses the use of the Internet through computers, smart phones, and other mobile devices.

In one case, for example, a Maine man hacked into a female victim's email account, found sexually explicit photographs of the victim there, and downloaded them to his phone. He then attempted to extort her into sending him even more sexually explicit images by threatening to publish explicit images on the internet – and distribute them to the victim's neighbors and work and social acquaintances. The offender pled guilty to violating section 2261A and was sentenced to serve 33 months in prison.

Until Congress passed the Violence Against Women Reauthorization Act of 2013, the federal prohibition on cyberstalking was limited by the statutory requirement that the stalker and the victim be in different states. In VAWA 2013, Congress revised the statute to bring it in line with other threatening statutes and permit federal prosecutors to pursue cyberstalking cases involving use of any electronic system of interstate commerce, regardless of where the victim and offender reside.

Closing

I appreciate the opportunity to share information with you about some of the challenges that the Department sees as society's use – and misuse-- of technology, including smart phones, tablets and laptops, continues to grow, and how the Department works to protect victims when those devices become another tool in the arsenal of stalkers. I look forward to continuing to work with the Congress as it considers these important issues.

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

S. 2171

THE LOCATION PRIVACY PROTECTION ACT OF 2014

Before the

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE FOR PRIVACY, TECHNOLOGY AND THE LAW

Washington, D.C.

June 4, 2014

I. Introduction

Chairman Franken, Ranking Member Flake, and members of the Subcommittee, my name is Jessica Rich, and I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate this opportunity to appear before you today to discuss the Commission's efforts to protect the privacy of consumers' geolocation information and to offer initial views on the draft Location Privacy Protection Act of 2014 ("LPPA").

The LPPA addresses an important issue for the Commission, as reflected in its enforcement, policymaking, and consumer and business education efforts over a number of years: protecting the privacy of consumers' geolocation information.

This testimony first broadly discusses why precise location information is sensitive personal information and how geolocation data is used increasingly in products and services offered to consumers. Second, it highlights the Commission's recent law enforcement actions involving geolocation information. Third, it discusses the Commission's studies, workshops, and reports addressing geolocation privacy on mobile devices. Next, it describes the Commission's efforts to educate both businesses and consumers about the importance of reasonable privacy controls and protections for geolocation information. It concludes by providing some specific comments on the LPPA.

II. The Sensitivity of Geolocation Information

The mobile marketplace has experienced remarkable growth, with new products and services offered every day, many of which rely on consumers' geolocation information. Products and services that use geolocation information make consumers' lives easier and more

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any Commissioner.

efficient.[2] For example, consumers can get turn-by-turn directions to their destinations, find the closest bank when they are far from home, and host impromptu gatherings with friends who have "checked-in" at a certain restaurant or bar.[3]

At the same time, because geolocation information can reveal a consumer's movements in real time, as well as provide a detailed, comprehensive record of a consumer's movements over time, use of this sensitive information can raise privacy concerns.[4] Geolocation information can divulge intimately personal details about an individual. Did you visit an AIDS clinic last Tuesday? What place of worship do you attend? Were you at a psychiatrist's office last week? Did you meet with a prospective business customer?[5] Businesses can use consumers' geolocation information to build profiles of a customer's activities over time and may put the information to unanticipated uses.[6]

Sensitive geolocation information could end up in the wrong hands in a number of ways, including by being sold to companies who then use it to build profiles with other sensitive

---

[2] A number of the most popular mobile device applications ("apps") use geolocation for certain features, such as mapping and geotagging photos. *See* Matt Patronzio, *The 10 Most Popular Smartphone Apps in the U.S.* (April 3, 2014), *available at* http://mashable.com/2014/04/03/popular-apps-chart/.

[3] *See, e.g.*, Government Accountability Office, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy* ("GAO Mobile Device Location Report") (Sept. 2012), at 13-15, *available at* http://www.gao.gov/assets/650/648044.pdf (noting diverse array of services that make use of geolocation information for the benefit of consumers).

[4] Federal Trade Commission, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Privacy Report") (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[5] *See, e.g.*, Andrew J. Blumberg and Peter Eckersley, "On Locational Privacy, and How to Avoid Losing it Forever," Electronic Frontier Foundation (Aug. 3, 2009), *available at* https://www.eff.org/wp/locational-privacy.

[6] *See* Elizabeth Dwoskin, *What Secrets Your Phone Is Sharing About You; Businesses Use Sensors to Track Customers, Build Shopper Profiles*, WALL ST. J. (Jan. 13, 2014), *available at* http://online.wsj.com/news/articles/SB10001424052702303453004579290632128929194; Leslie Scism, *State Farm Is There: As You Drive. Insurers Use Big Data to Track Drivers, Offering Discounts as Lure, But Privacy Advocates See Dangers*, WALL ST. J. (Aug. 4, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887323420604578647950497541958 (reporting that some insurance companies are starting to provide voluntary services that use geolocation and other data points to offer better insurance rates based, at least in part, on good driving behavior).

information, such as medical conditions or religious affiliation, without consumers' knowledge or consent, by being accessed by hackers, or by being collected through surreptitious means such as "stalking apps."[7] Given that geolocation information reveals personal information – such as where individuals live, work, or attend school – a cybercriminal could use geolocation information to facilitate social engineering or install malware or key loggers to steal a user's identity or mine credit card numbers or Social Security numbers.[8] Moreover, after obtaining an individual's geolocation information, criminals could use it to identify the individual's present or future location, thus enabling them to cause harm to an individual or his or her property, ranging from burglary and theft, to stalking, kidnapping, and domestic violence.[9]

In 2012, the Government Accountability Office ("GAO"), in a report on mobile location data, discussed consumer benefits that come with use of geolocation information – such as services that provide local weather forecasts, navigation, and retail locations – but also warned that allowing companies to access and use consumers' geolocation data exposes consumers to privacy risks, including disclosing data to unknown third parties for unspecified uses, consumer tracking, identity theft, threats to personal safety, and surveillance.[10] Likewise, many consumers are concerned about the privacy of their location data. For example, one recent study found that

---

[7] Stalking apps, which have been the subject of testimony before this Committee in the past, are apps installed on a mobile device that allow a person to monitor the device user's communications and location. Such apps can create serious safety risks for domestic violence victims whose call records, text messages, and geolocation information can be tracked by their abusers. In a similar context, the Commission has taken action against marketers of keylogger software that could, without the computer owner's consent or knowledge, record every keystroke typed on a computer. *See FTC v. CyberSpy*, No. 6:08-cv-1872-ORL-31GLK (M.D. Fla. 2010), *available at* http://www.ftc.gov/enforcement/cases-proceedings/082-3160/cyberspy-software-llc-trace-r-spence.

[8] *See* ISACA, Geolocation: Risk, Issues and Strategies (Sept. 2011), at 8, *available at* http://www.isaca.org/groups/professional-english/wireless/groupdocuments/geolocation_wp.pdf.

[9] *See id.*

[10] *See* GAO Mobile Device Location Report, *supra* note 3, at 9, 13-15.

nearly three quarters of consumers surveyed were reluctant to enable location tracking on their phones due to privacy concerns.[11]

III. Enforcement

The FTC is first and foremost a civil law enforcement agency. Absent specific laws that protect geolocation information, the FTC has used its core consumer protection authority – Section 5 of the FTC Act – to enforce against unfair or deceptive practices.[12] A company acts deceptively if it makes materially misleading statements or omissions.[13] A company engages in unfair acts or practices if its practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[14] The Commission has used its enforcement authority under Section 5 to take action against companies engaged in unfair or deceptive practices involving geolocation information.

Last month, Snapchat, the developer of a popular mobile messaging app, entered into a settlement with the Commission.[15] According to the Commission's complaint, Snapchat made

---

[11] TRUSTe, *2014 U.S. Consumer Confidence Privacy Report* (Jan. 28, 2014), *available at* http://www.truste.com/about-TRUSTe/press-room/news_us_truste_reveals_consumers_more_concerned_about_data_collection; *see also* NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), *available at* http://www.nielsen.com/us/en/newswire/2011/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location.html (finding a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device).

[12] 15 U.S.C. § 45(a). In addition, the Commission enforces the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501(8)(b), and its implementing rule, 16 C.F.R. Part 312, which includes "geolocation information" in the definition of "personal information" that child-directed websites and online services, as well as those with actual knowledge they are dealing with a child, may only collect with parental consent.

[13] *See* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[14] *See* 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[15] *Snapchat, Inc.*, No. 1323078 (F.T.C. May 8, 2014) (proposed consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

multiple misrepresentations to consumers about the fundamental features of its app, including the privacy features for which it was known. The FTC alleged that Snapchat deceived consumers by promising that photo and video messages sent through the service would disappear, misrepresenting the amount of personal data it collected, and misrepresenting the security measures taken to protect that data from misuse and unauthorized disclosure. Among other things, the Commission's complaint alleged that Snapchat transmitted geolocation information from users of its Android app, even though its privacy policy claimed that it did not track users or access such information. The Commission's proposed consent order prohibits Snapchat from misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users' information. In addition, the proposed order requires the company to implement a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.

In another case involving a mobile app developer, the FTC alleged that the developer of a flashlight app – one of the most popular apps for the Android platform, downloaded tens of million times – deceptively failed to disclose that the app transmitted the device's location, device ID, and other device data to third parties, including mobile advertising networks ("ad networks").[16] The company's privacy policy stated that it would collect "diagnostic, technical, and related" information about consumers' devices for such internal purposes as product support and software updates. The policy, however, failed to mention that the company would collect the devices' precise geolocation and persistent identifier and send them to third parties, such as ad networks. In addition, the complaint alleged that the company deceived consumers by presenting them with an option not to have their data collected or used, but nevertheless collected

[16] *Goldenshores Technologies, LLC*, No. C-4446 (F.T.C. Mar. 31, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter.

and shared the data automatically, thus rendering the option meaningless. The company and its manager agreed to an order that prohibits them from misrepresenting how consumers' information is collected and shared and how much control consumers have over the way their information is used. The respondents are also required to provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used, and shared, and the respondents must obtain consumers' affirmative express consent before doing so.

Finally, in a series of settlements with national rent-to-own retailer, Aaron's, a company that leased software to Aaron's, and seven of Aaron's franchisees, the FTC alleged that the companies' installation and use of software on rental computers that secretly monitored and tracked consumers ran afoul of Section 5.[17] The software could log key strokes, capture screen shots, and take photographs using a computer's webcam, all unbeknownst to users. The FTC alleged that the information collected by the software revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to

[17] *Aaron's, Inc.*, No. C-4442 (F.T.C. Mar. 10, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter; *DesignerWare, LLC*, No. C-4390 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter; *Aspen Way Enterprises, Inc.*, No. C-4392 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/aspen-way-enterprises-inc-matter; *Watershed Development Corp.*, No. C- 4398 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/watershed-development-corp-matter; *Showplace, Inc.*, No. C- 4397 (F.T.C April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/showplace-inc-matter; *J.A.G. Rents, LLC*, No. C- 4395 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/jag-rents-llc-also-dba-colortyme-matter; *Red Zone Investment Group, Inc.*, No. C-4396 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/red-zone-investment-group-inc-matter; *B. Stamper Enterprises, Inc.*, No. C-4393 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/b-stamper-enterprises-inc-matter; *C.A.L.M. Ventures, Inc.*, No. C-4394 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/calm-ventures-inc-matter.

doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home. In its complaints against the companies, the FTC alleged that gathering and disclosing personal information about renters was unfair and violated the FTC Act. With respect to geolocation information, the FTC alleged that installing location tracking software on rented computers without consent from the computers' renters, tracking the geolocation of computers without notice to the computer users, and disclosing that location information to rent-to-own store licensees, caused or was likely to cause substantial injury to consumers that could not be reasonably avoided and was not outweighed by countervailing benefits to consumers or competition. Among other things, the settlement orders prohibit the companies from using monitoring software and prohibit the use of geolocation tracking without consumer consent and notice, except in cases where the device has been stolen.

IV. Policy Initiatives

In addition to the Commission's enforcement activities involving geolocation information, the Commission has conducted studies, held workshops, and issued reports on mobile privacy disclosures, mobile apps directed to kids, and other topics that elucidate best practices for companies collecting, using, and sharing information such as geolocation information.

FTC staff issued two reports about the disclosures provided in mobile apps for children: *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, published in February 2012,[18] and *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, published in

[18] FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf ("First Kids' App Report").

December 2012.[19] The reports discussed what data is collected by children's apps and how it is shared, and urged industry to take steps to provide parents easier access to information about the data apps are collecting and sharing. In the February 2012 report, FTC staff surveyed the types of apps offered to children in the Apple App Store and the Android Market, and evaluated the disclosures provided to users, interactive features such as connectivity with social media, and the ratings and parental controls offered for such apps. The report noted that mobile apps can capture a broad range of user information from a mobile device automatically, including the user's precise geolocation, phone number, list of contacts, call logs, unique identifiers, and other information stored on the device. After examining the disclosures of 400 apps, FTC staff concluded that there was a lack of information available to parents prior to downloading mobile apps for their children. This was particularly problematic given the breadth of and sensitivity of the personal information apps can capture. The report called on industry to provide greater transparency about their data practices.

In December 2012, FTC staff released the results of a follow-up survey that examined whether app disclosures had improved, and whether and how apps were sharing certain types of data with third parties.[20] The survey results showed, in many instances, that apps still failed to give parents basic information about the privacy practices and interactive features of mobile apps aimed at kids. The staff found that many apps failed to provide any information about the data collected through the app, let alone the types of data collected, the purpose of the collection, and who could access to the data. Even more troubling, the results showed that many of the apps

[19] FTC Staff, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf ("Second Kids' App Report").

[20] The study was conducted in the Commission's mobile technology laboratory, which contains a variety of mobile devices utilizing different platforms and carriers, as well as software and equipment that permit FTC investigators to collect and preserve evidence and conduct research into a wide range of mobile issues, including those related to consumer privacy.

shared certain information – such as device ID, geolocation, or phone number – with third parties without disclosing that fact to parents.[21] The report urged all entities in the mobile app industry to accelerate efforts to ensure that parents have the key information they need to make decisions about the apps they download for their children.

Expanding on prior work regarding mobile disclosures, in February 2013, FTC staff issued *Mobile Privacy Disclosures: Building Trust Through Transparency.*[22] This staff report made recommendations for all players in the mobile marketplace – platforms, app developers, ad networks and analytics companies, and trade associations – to ensure that consumers get timely, easy-to-understand disclosures about what data companies collect and how that data is used. The report specifically discussed the need for just-in-time disclosures to consumers and obtaining affirmative express consent before allowing access to sensitive information like geolocation.

The FTC continually assesses new developments and emerging trends and threats in the privacy area. Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy implications of a number of new technologies in the marketplace.[23] The first seminar, held in February, included a panel of industry, technical experts, and privacy advocates and examined

---

[21] Although the results found that only 3% (12) of the apps in the study transmitted a user's geolocation, in every instance where an app transmitted geolocation, it also transmitted the user's device ID. The device ID is a persistent identifier associated with a particular mobile device. As a result, third parties, such as ad networks, that received this geolocation data could potentially add it to any data previously collected through other apps running on the same device. For example, FTC staff found that one ad network received information from 31 different apps. Two of these apps transmitted geolocation to the ad network along with a device identifier, and the other 29 apps transmitted other data (such as app name, device configuration details, and the time and duration of use) in conjunction with a device ID. The ad network could thus link the geolocation information obtained through the two apps to all the other data collected through the other 29 apps by matching the unique, persistent device ID. Second Kids'App Report, *supra* note 19, at 10.

[22] FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf ("Mobile Privacy Disclosures Report").

[23] Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues* (Dec. 2, 2013) *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

the privacy and security implications of mobile device tracking, where retailers and other companies use technology that can reveal information about consumers' visits to and movements within a location.[24] The seminar examined how mobile device tracking technologies work and how they are used; potential benefits to consumers, including improving customer flow through a store and efficient shopping and checkout; and privacy concerns, such as the lack of transparency of data collection, inability to opt-out, and potential profiling of customers' buying habits and geolocation information. FTC staff solicited public comments after the seminar, and a report summarizing the findings is forthcoming.

V. Consumer Education and Business Guidance

The Commission has long viewed consumer education and business guidance as an essential part of its consumer protection mission. In addition to our enforcement and policy work, the Commission educates consumers and businesses about protecting the privacy of consumers' geolocation information. The Commission has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy and makes its guidance materials available online. The FTC recently released an updated version of "Net Cetera: Chatting with Kids About Being Online," our guide to help parents and other adults talk to kids about being safe, secure, and responsible online.[25] This new version deals with such topics as mobile apps and privacy, public Wi-Fi security, text message spam, and updated guidance on the Commission's COPPA Rule. Likewise, the FTC's Consumer Information website contains numerous guides on privacy and security topics salient to

[24] *See* Spring Privacy Series, *Mobile Device Tracking* (Feb. 19, 2014) *available at* http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.
[25] Net Cetera: Chatting with Kids About Being Online (Jan. 2014), *available at* https://www.consumer.ftc.gov/articles/pdf-0001-netcetera.pdf.

consumers, including a guide on understanding mobile apps and what information they collect from consumers.[26]

The Commission also has released guidance directed to businesses operating in the mobile arena to help educate them on best practices to handle sensitive information, such as geolocation information. The FTC published a guide, "Marketing Your Mobile App: Get It Right from the Start," to help mobile app developers observe truth-in-advertising and basic privacy principles when marketing new apps.[27] Likewise, because mobile apps and devices often rely on sensitive consumer data, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps.[28]

In addition to issuing written materials, FTC staff also has actively worked to educate mobile companies directly. For example, staff members have spoken at numerous meetings of mobile app developers to urge them to move forward on their efforts to improve transparency and address consumer privacy issues. The Commission's hope is that these tools provide guidance to companies, large and small, on how to prioritize the privacy and security of consumer information as they develop new products and services.

VI. The Location Privacy Protection Act of 2014

The Commission supports the goals of the LPPA, which chiefly seeks to improve the transparency of geolocation services and give consumers greater control over the collection of their geolocation information. Currently, in the commercial sphere, there are various laws that

---

[26] Understanding Mobile Apps (Sept. 2011), *available at* http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps.

[27] Marketing Your Mobile App: Get It Right from the Start (April 2013), *available at* http://www.business.ftc.gov/documents/bus81-marketing-your-mobile-app.

[28] Mobile App Developers: Start with Security (Feb. 2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

protect other types of sensitive information, for example: the Gramm-Leach-Bliley Act[29] protects financial information; the Fair Credit Reporting Act[30] protects information used for consumer reporting purposes; and the Health Insurance Portability and Accountability Act[31] protects personal health information. The LPPA represents an important step forward in protecting consumers' sensitive geolocation information.

In particular, this testimony highlights three important LPPA provisions that are consistent with the Commission's views. First, the bill defines "geolocation information" as information that is "sufficient to identify the street name and name of the city or town" in which a device is located. This definition is consistent in many respects with the Commission's COPPA Rule. The COPPA Rule requires parental consent for the collection of children's "geolocation information," that is "sufficient to identify street name and name of city or town."[32] The Commission supports the use of a consistent definition in the LPPA. Second, the LPPA requires that an entity collecting consumer geolocation information disclose its collection of such information. The Commission has recommended that companies make their data collection practices more transparent to consumers.[33] The disclosure mechanism outlined in the LPPA is an important step forward on transparency concerning the collection of geolocation information. Third, the LPPA requires affirmative express consent from consumers before a covered entity

---

[29] 15 U.S.C. §§ 6801-6827.
[30] 15 U.S.C. §§ 1681-1681x.
[31] 42 U.S.C. 1301 *et seq.*; *see also* 45 C.F.R Parts 160, 162 & 164.
[32] 16 C.F.R. Part 312.2.
[33] *See* Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; First Kids' App Report, *supra* note 18; Second Kids' App Report, *supra* note 19; Mobile Privacy Disclosures Report, *supra* note 22.

may knowingly collect or disclose geolocation information, and the Commission supports that approach.[34]

The LPPA gives the Department of Justice rulemaking authority, in consultation with the FTC, as well as sole enforcement authority. As the federal government's leading privacy enforcement agency, we recommend that the Commission be given rulemaking and enforcement authority with regard to the civil provisions of the LPPA, with DOJ exercising enforcement authority for the criminal provisions.

VII. Conclusion

Thank you for the opportunity to provide the Commission's views on privacy and geolocation information. The Commission is committed to protecting the privacy of consumers' geolocation information and we look forward to continuing to work with the Committee and Congress on this critical issue.

[34] *See* Privacy Report, *supra* note 4, at 59 (stating that precise geolocation is sensitive information that requires extra protections, including giving consumers an opportunity to provide affirmative express consent before it is collected or used).; Mobile Privacy Disclosures Report, *supra* note 22, at 15-16 (same).

PREPARED STATEMENT OF MARK L. GOLDSTEIN

United States Government Accountability Office

Testimony

Before the Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, United States Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Wednesday, June 4, 2014

CONSUMERS' LOCATION DATA

Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers

Statement of Mark L. Goldstein, Director, Physical Infrastructure Issues

GAO-14-649T

GAO Highlights

Highlights of GAO-14-649T, a testimony before the Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, United States Senate

Why GAO Did This Study

Smartphones and in-car navigation systems give consumers access to useful location-based services, such as mapping services. However, questions about privacy can arise if companies use or share consumers' location data without their knowledge.

Several agencies have responsibility to address consumers' privacy issues, including FTC, which has authority to take enforcement actions against unfair or deceptive acts or practices, and NTIA, which advises the President on telecommunications and information policy issues.

This testimony addresses (1) companies' use and sharing of consumers' location data, (2) consumers' location privacy risks, and (3) actions taken by selected companies and federal agencies to protect consumers' location privacy.

This testimony is based on GAO's September 2012 and December 2013 reports on mobile device location data and in-car location-based services and December 2012 and May 2013 updates from FTC and NTIA on their actions to respond to the 2012 report's recommendations.

What GAO Recommends

GAO made recommendations to enhance consumer protections in its 2012 report. GAO recommended, for example, that NTIA develop goals, milestones, and measures for its stakeholder initiative. NTIA stated that taking such actions is the role of the stakeholders and that its stakeholders had made progress in setting goals, milestones, and performance measures. GAO will continue to monitor this effort.

View GAO-14-649T. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

June 2014

CONSUMERS' LOCATION DATA

Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not Be Clear to Consumers

What GAO Found

Fourteen mobile industry companies and 10 in-car navigation providers that GAO examined in its 2012 and 2013 reports—including mobile carriers and auto manufacturers with the largest market share and popular application developers—collect location data and use or share them to provide consumers with location-based services and improve consumer services. For example, mobile carriers and application developers use location data to provide social networking services that are linked to consumers' locations. In-car navigation services use location data to provide services such as turn-by-turn directions or roadside assistance. Location data can also be used and shared to enhance the functionality of other services, such as search engines, to make search results more relevant by, for example, returning results of nearby businesses.

While consumers can benefit from location-based services, their privacy may be at risk when companies collect and share location data. For example, in both reports, GAO found that when consumers are unaware their location data are shared and for what purpose data might be shared, they may be unable to judge whether location data are shared with trustworthy third parties. Furthermore, when location data are amassed over time, they can create a detailed profile of individual behavior, including habits, preferences, and routes traveled—private information that could be exploited. Additionally, consumers could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods or in a way that links the data to individual consumers. Companies can anonymize location data that they use or share, in part, by removing personally identifying information; however, in its 2013 report, GAO found that in-car navigation providers that GAO examined use different de-identification methods that may lead to varying levels of protection for consumers.

Companies GAO examined in both reports have not consistently implemented practices to protect consumers' location privacy. The companies have taken some steps that align with recommended practices for better protecting consumers' privacy. For example, all of the companies examined in both reports used privacy policies or other disclosures to inform consumers about the collection of location data and other information. However, companies did not consistently or clearly disclose to consumers what the companies do with these data or the third parties with which they might share the data, leaving consumers unable to effectively judge whether such uses of their location data might violate their privacy. In its 2012 report, GAO found that federal agencies have taken steps to address location data privacy through educational outreach events, reports with recommendations to protect consumer privacy, and guidance for industry. For example, the Department of Commerce's National Telecommunications and Information Administration (NTIA) brought stakeholders together to develop codes of conduct for industry, but GAO found this effort lacked specific goals, milestones, and performance measures, making it unclear whether the effort would address location privacy. Additionally, in response to a recommendation in GAO's 2012 report, the Federal Trade Commission (FTC) issued guidance in 2013 to inform companies of the Commission's views on the appropriate actions mobile industry companies should take to disclose their privacy practices and obtain consumers' consent.

Chairman Franken, Ranking Member Flake, and Members of the Subcommittee,

I am pleased to be here today to discuss our work on location privacy issues. Location-based services in smartphones and cars provide consumers with navigation tools and information relevant to their surroundings based on increasingly precise information about the consumer's location as determined by Global Positioning System (GPS) and other methods. In offering such services, companies can collect and retain precise data about consumers' locations. Privacy advocacy groups and policy makers have questioned whether location data that are collected and used by these companies pose privacy risks. Specifically, they have noted that location data can be used for purposes other than to provide services to the consumer, such as selling the data to others for marketing. They have also said that location data can be used to track consumers, which can in turn be used to steal their identity, stalk them, or monitor them without their knowledge. In addition, they have said that location data can be used to infer other sensitive information about individuals such as their religious affiliation or political activities.

My statement today highlights our work on: (1) companies' use and sharing of consumers' location data, (2) consumers' location privacy risks, and (3) actions taken by selected companies and federal agencies to protect consumers' location privacy. For this statement, we drew primarily from our reports on mobile device location data and in-car location-based services issued in September 2012 and December 2013, respectively.[1] For those reports, we examined privacy policies and other documentation and interviewed representatives of selected mobile industry companies and in-car navigation service companies.[2] We analyzed whether the

[1]GAO, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO-12-903 (Washington, D.C.: Sept. 11, 2012) and *In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers*, GAO-14-81 (Washington, D.C.: Dec. 6, 2013).

[2]Specifically, for the 2012 mobile device report, we examined 14 mobile industry companies, comprising mobile carriers, operating system developers, and smartphone manufacturers that accounted for the largest market shares in the United States, and developers of applications that were the most popular at the time. For the 2013 in-car location-based services report, we examined 10 in-car navigation service companies, comprising auto manufacturers and portable navigation device companies that had the largest market share in the United States, and developers of widely used map and navigation applications.

selected companies' privacy policies and reported practices aligned with recommended privacy practices we identified based on our analysis of information from industry associations and privacy advocacy groups. We also reviewed documents and interviewed officials from federal agencies. Additionally, in December 2012 and May 2013, we followed up on agency actions to respond to recommendations we made in the 2012 report. Our September 2012 and December 2013 reports contain more detailed explanations of the methods used to conduct our work. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Consumers may access location-based services through smartphones or from in-car location-based services. Four types of companies are primarily responsible for smartphone products and services in the United States: mobile carriers, such as AT&T and Verizon; developers of operating systems, such as Apple's iPhone iOS and Google's Android; manufacturers, such as HTC and Samsung; and developers of applications such as games like Angry Birds, social networking applications like Facebook, or navigation tools like Google Maps. We refer to these companies as mobile industry companies. In-car location-based services are delivered by in-car communications systems known as "telematics" systems,[3] portable navigation devices, and map and navigation applications for mobile devices.

Companies can obtain location data in various ways. Mobile devices and in-car navigation devices determine location information through methods such as cell tower signal-based technologies, Wi-Fi Internet access point technology, crowd-sourced positioning, and GPS technology. Assisted-GPS (A-GPS), a hybrid technology that uses more than one data collection methodology, is also widely used. For example, companies such as Google and Apple use customer data to compile large databases

[3]Telematics systems use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider.

of cell tower and Wi-Fi access points. Non-carriers use these crowd-sourced location maps to determine location by analyzing which cell tower and Wi-Fi signals are received by a device. Consumers' location data are transmitted over the cellular network or Wi-Fi access points to companies providing the services. These location data may then be shared with third parties for various uses. For example, companies may choose to partner with third parties to provide a specific location-based service, such as real-time traffic information.

Several agencies have responsibility to address consumers' privacy and create related guidance. The Federal Trade Commission (FTC) has authority to enforce action against unfair or deceptive acts or practices of companies; the Federal Communications Commission (FCC) has regulatory and enforcement authority over mobile carriers; and the Department of Commerce's (Commerce) National Telecommunications and Information Administration (NTIA) advises the President on telecommunications and information policy issues. Additionally, the Department of Justice disseminates guidance on how law enforcement might request electronic evidence, such as a person's current or historical location data.

Companies Primarily Collect and Share Location Data to Provide and Improve Consumer Services

Representatives from mobile industry companies we spoke to for the September 2012 report and in-car navigation service companies we spoke to for the December 2013 report told us they primarily collect and share location data to provide location services and to improve those services. Mobile carriers and application developers offer a diverse array of services that use location information, such as services providing navigation and social networking services that are linked to consumers' locations. To provide these services, carriers and developers need to quickly and accurately determine location. Location data can also be used to enhance the functionality of other services that do not need to know the consumer's location to operate. Search engines, for example, can use location data as a frame of reference to return results that might be more relevant. For instance, if a consumer were to search for a pizza restaurant using a location-aware search engine, the top result may be a map of nearby pizza restaurants instead of the homepage of a national chain. In-car location services use location data to provide services such as turn-by-turn directions or roadside assistance. Representatives from both mobile industry companies and in-car navigation services companies told us they also use location data to improve the accuracy of their services. Representatives from some in-car navigation service companies said they share aggregated location data associated with traffic flows with third

parties to augment and improve the accuracy of real-time traffic services provided to consumers.

Additionally, as we reported in 2012, mobile industry companies can use and sell location data to target the advertising that consumers receive through mobile devices. Doing so may make an advertisement more relevant to a consumer than a non-targeted advertisement, boosting advertising revenue. Advertising is particularly important to application developers, as many developers give their products away and rely on advertising to consumers through free applications for revenue. Companies may also aggregate and store individual consumer data to create consumer profiles. Profiles can be used to tailor marketing or service performance to an individual's preferences.

Mobile industry companies and providers of in-car location services must also share consumer location data if a court finds that the information is warranted for law enforcement purposes. Because consumers generally carry their mobile devices with them, law enforcement can use device location data to determine the consumer's location. Because of this correlation, location data are valuable to law enforcement for tracking the movements of criminal suspects. Mobile carriers must comply with court orders directing the disclosure of historical location data (i.e., where the device was in the past) and in certain circumstances, real-time location data (i.e., where the device is now).[4]

Companies' Collection and Sharing of Location Data May Put Consumers' Privacy at Risk

Although consumers can benefit from location-based services designed to make their lives easier, consumers also expose themselves to privacy risks when they allow companies to access their location data. In some cases, consumers of location-based services may be unaware that companies share their location data for purposes other than providing those services. As we stated in our September 2012 and December 2013 reports, these privacy risks include, but are not limited to the following:

Disclosure to Unknown Third Parties for Unspecified Uses: According to privacy advocates, when a consumer agrees to use a service that accesses location data, the consumer is unlikely to know how

[4]However, for companies that do not retain personally identifiable location data, there are no data for law enforcement to use.

his or her location data may be used in ways beyond enabling the service itself. For example, location data may be shared with third parties unknown to the consumer. Because consumers do not know who these entities are or how they are using consumers' data, consumers may be unable to judge whether they are disclosing their data to trustworthy entities. Third parties that receive shared location information may vary in the levels of security protection they provide. If any of these entities has weak system protections, there is an increased likelihood that the information may be compromised.

Tracking Consumer Behavior: When location data are collected and shared, these data could be used in ways consumers did not intend, such as to track their travel patterns or to target consumers for unwanted marketing solicitations. Since consumers often carry their mobile devices with them and can use them for various purposes, location data along with data collected on the device may be used to form a comprehensive record upon which an individual's activities may be inferred. Amassing such data over time allows companies to create a richly detailed profile of individual behavior, including habits, preferences, and routines—private information that could be exploited. Consumers may believe that using these personal profiles for purposes other than providing a location-based service constitutes an invasion of privacy, particularly if the data are used contrary to consumers' expectations and results in unwanted solicitations or other nuisances.

Identity Theft: Criminals can use location data to steal identities when location data are disclosed, particularly when they are combined with other personal information. The risk of identity theft grows whenever entities begin to collect data profiles, especially if the information is not maintained securely. By illicitly gaining access to these profiles, criminals acquire information such as a consumer's name, address, interests, and friends' and co-workers' names. In addition, a combination of data elements—even elements that do not by themselves identify anyone, such as individual points of location data—could potentially be used in aggregate to identify or infer a consumer's behavior or patterns. Such information could be used to discern the identity of an individual. Furthermore, keeping data long-term, particularly if it is in an identifiable profile, increases the likelihood of identity theft.

Personal Security: Location data may be used to form a comprehensive record of an individual's movements and activities. If disclosed or posted, location data may be used by criminals to identify an individual's present or probable future location, particularly if the data also contain other

personally identifiable information. This knowledge may then be used to harm the individual or his property through, for instance, stalking or theft. Access to location information also raises child safety concerns as more children access mobile devices and location-based services. According to the American Civil Liberties Union (ACLU), location updates that consumers provide through social media have been linked to robberies, and GPS technology has been involved in stalking cases.

Surveillance: Law enforcement agencies can obtain location data through various methods, such as a court order, and such data can be used as evidence. However, according to a report by the ACLU, law enforcement agents could potentially track innocent people, such as those who happened to be in the vicinity of a crime or disturbance.[5] Consumers generally do not know when law enforcement agencies access their location data. In addition to information related to a crime, the location data collected by law enforcement may reveal potentially sensitive destinations, such as medical clinics, religious institutions, courts, political rallies, or union meetings.

Selected Companies Have Not Consistently Implemented Practices to Protect Consumers' Location Privacy; Federal Agencies Have Taken Actions but Federal Privacy Law Is Not Comprehensive

[5]American Civil Liberties Union of Northern California. *Location-Based Services: Time for a Privacy Check-in* (San Francisco, Calif.: November 2010).

Private Sector Entities Have Implemented Some Recommended Practices to Protect Consumers' Location Privacy, but Not Consistently

Industry and privacy advocacy groups have recommended practices for companies to follow in order to better protect consumers' privacy while using their personal information. These recommended practices include: (1) providing disclosures to consumers about data collection, use, and sharing; (2) obtaining consent and providing controls over location data; (3) having data retention practices and safeguards; and (4) providing accountability for protecting consumers' data. For the September 2012 report, we examined 14 mobile industry companies, and the for December 2013 report, we examined 10 in-car navigation services companies.[6] These companies have taken steps that are consistent with some, but not all, of the recommended practices:

Disclosures: All of the companies we examined for both reports have privacy policies, terms-of-service agreements, or other practices—such as on-screen notifications—to notify consumers that they collect location data and other personal information. However, some companies have not consistently or clearly disclosed to consumers what they are doing with these data or which third parties they may share them with. For example, most of the in-car navigation service companies we examined for the 2013 report provide broadly worded reasons for collecting location data that potentially allow for unlimited data collection and use. One of those company's terms of service states that the provided reasons for location data collection were not exhaustive. Furthermore, about half of the in-car navigation service companies' disclosures allow for sharing for location data when they are de-identified, but most of these companies' disclosures did not describe the purposes for sharing such data.

Consent and Controls: All of the companies we examined for both reports indicated they obtain consumer consent to collect location data and obtain this consent in various ways, some of which are more explicit than others. Companies also reported providing methods for consumers to control collection and use of location data, but the methods and amount of control varied. For example, most of the 14 mobile industry companies we examined for the 2012 report indicated that consumers could control smartphones' use of their location data from the phone; however, the ability to control this varied by operating system, with some providing more options. For example, the iPhone iOS operating system

[6]One company that is both an operating system developer and a provider of navigation services was examined for both the 2012 and 2013 reports.

displays a pop-up window the first time a consumer activates a new application that includes location-based services. The pop-up states that the application seeks to use the consumer's location and allows the consumer to accept or decline at that time. Similarly, Android smartphones notify consumers that an application will use location data at the time a consumer downloads a new application and seeks consumer consent through this process. Some in-car navigation systems we examined for the 2013 report use similar methods to notify consumers that they will collect location data to provide services. In contrast, other in-car navigation services obtain consent when a consumer purchases a vehicle. According to one privacy group we met with, if consent is obtained in this manner, consumers may not be as likely to review a company's stated privacy practices because they may be a part of a larger set of documentation about the vehicle. Additionally, none of the 10 in-car navigation service companies we examined allow consumers to delete the location data that are, or have been, collected.[7]

Retention and Safeguards: Officials from most of the companies we interviewed for the 2012 and 2013 reports said they kept location data only as long as needed for a specific purpose; however, in some cases, this could mean keeping location data indefinitely. Most of the privacy policies of the 14 mobile services companies we examined did not state how long companies keep location data, and there was wide variation in how long in-car navigation services companies retain vehicle-specific or personally identifiable location data when a customer requests services, ranging from not at all to up to 7 years. All the mobile industry companies we examined reported ways they safeguard consumers' personal information. However, in some cases, it was not clear whether these protections covered location data, since some privacy policies did not state whether location was considered a form of personal information. Thus it was unclear whether stated safeguards for personal information applied to location data.

As we reported in 2013, companies may safeguard location data that they use or share, in part, by de-identifying them, but companies we examined used different de-identification methods. De-identified data are stripped of

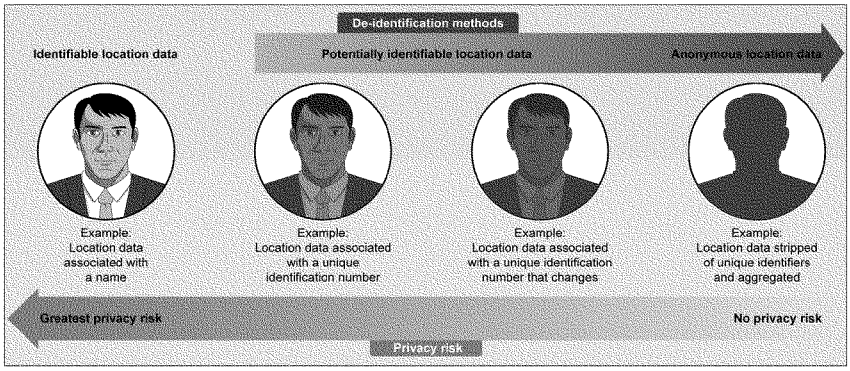
[7]We did not examine this specific issue in our 2012 report on mobile devices.

personally identifiable information.[8] The de-identification method a company uses affects the extent to which consumers may be re-identified and exposed to privacy risks. Location data that are collected along with a consumer's name or other identifying information are, by definition, personally identifiable data and present the greatest privacy risks to consumers because a consumer's identity is known. Privacy risks decrease when companies de-identify location data, but the level of risk falls on a spectrum depending on how easy it is to re-identify consumers. For example, de-identifying location data with unique identification numbers prevents the direct association of location data with a specific vehicle or individual. However, if the same identification number is re-used for the same consumer on multiple trips, then the consumer's history or patterns can potentially be discerned. Conversely, consumers face little to no privacy risks when location data are stripped of any identification numbers and aggregated with other consumers' data because the data are anonymous, meaning that the data cannot be linked to an individual at all (see fig. 1). All of the in-car navigation service companies we examined stated in their disclosures, or in interviews with us, that they use or share de-identified location data.[9]

[8]Personally identifiable information is information that is linked to a specific individual and can be used to locate or identify that person; this information includes an individual's name, aliases, Social Security number, and biometric records.

[9]We did not specifically assess the use or sharing of de-identified location data among the mobile industry companies.

Figure 1: Examples of De-Identification Methods and Privacy Risk Associated with Location-Based Data



Source: GAO.

Accountability: We reported in 2012 and 2013 that companies' accountability practices varied. For example, all 10 of the in-car navigation services companies we examined for the 2013 report stated in their disclosures or in interviews with us that they take steps to protect location data that they share with third parties. Additionally, some mobile carriers we examined for the 2012 report said they use their contracts with third parties they share consumers' personal data with to require those third parties to adhere to industry recommended practices for location data. In the 2013 report, we found that while not disclosed to consumers, representatives of in-car navigation services companies said their employees must follow the companies' internal polices to protect data, including location data, and some of the representatives further explained that employees who violate such policies are subject to disciplinary action and possibly termination. Separately, representatives from one of the in-car navigation service companies told us that it had conducted an independent audit of its practices to provide reasonable assurance that it was in line with company privacy policies. Additionally, three of the mobile industry companies we examined for the 2012 report had their privacy practices certified by TRUSTe, a company that helps companies address privacy issues by certifying businesses' privacy programs.

Lacking clear information about how companies use and share consumers' location data, consumers deciding whether to allow companies to collect, use, and share data on their location would be unable to effectively judge whether their privacy might be violated.

Federal Agencies Have Taken Actions to Protect Consumer Privacy

In our September 2012 report on mobile device location data, we reported that federal agencies that have responsibility for consumer data privacy protection have taken steps to promote awareness of privacy issues, such as providing educational outreach and recommending actions aimed at improving consumer privacy.[10] For example, in February 2012, NTIA prepared a report for the White House on protecting privacy and promoting innovation in the global digital economy.[11] The report offered a framework and expectations for companies that use personal data. The framework includes a consumer privacy bill of rights, a multistakeholder process to specify how the principles in the bill of rights apply in particular business contexts, and effective enforcement. In February 2012, FTC issued a report on privacy disclosures for mobile applications aimed at children.[12] This report highlighted the lack of information available to parents prior to downloading mobile applications for their children and called on the mobile industry to provide greater transparency about their data practices. FTC also issued a consumer privacy report in March 2012 with recommendations for companies that collect and use consumer data, including location data.[13] Finally, the Department of Justice has

[10]In the 2012 report, we also reported on three regulatory actions in the area of protecting mobile location data.

[11]The White House, *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C.: Feb. 23, 2012).

[12]Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Washington, D.C.: February 2012).

[13]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: March 2012).

developed guidance on how law enforcement may obtain mobile location data.[14]

In our 2012 report, we concluded that NTIA and FTC could take additional actions to further protect consumers. For example, we found that NTIA had not defined specific goals, milestones, or performance measures for its proposed multistakeholder process, which consists of different groups involved with consumer privacy coming together to discuss relevant issues with the goal of developing codes of conduct for consumer privacy. Therefore, it was unclear whether the process would address location privacy. Consequently, we recommended that NTIA, in consultation with stakeholders in the multistakeholder process, develop specific goals, time frames, and performance measures for the multistakeholder process to create industry codes of conduct. In a December 2012 response to our report, the Department of Commerce (NTIA is an agency of Commerce) said it disagreed with this recommendation, stating that it is the role of the stakeholders, not the agency, to develop goals, time frames, and performance measures for the multistakeholder process. Additionally, the letter stated that stakeholders had made progress to develop their own goals, time frames, and performance measures for their efforts to create a code of conduct for mobile application transparency. We will continue to monitor NTIA's efforts in this area.

Additionally, we found that FTC had not issued comprehensive guidance to mobile industry companies with regard to actions companies should take to protect mobile location data privacy. Doing so could inform companies of FTC's views on the appropriate actions companies should take to protect consumers' mobile location privacy. We recommended that FTC consider issuing industry guidance establishing FTC's views of the appropriate actions mobile industry companies could take to protect mobile location data privacy. In February 2013, FTC issued a staff report on mobile privacy disclosures; the report provided guidance for mobile industry companies to consider when disclosing their information collection and use practices. In particular, the report suggested best practices for operating systems, application developers, advertising

[14]See, for example, Department of Justice, Executive Office for United States Attorneys. *Obtaining and Admitting Electronic Evidence* (Washington, D.C.: 2011) and Department of Justice, *Computer Crime and Intellectual Property Section Criminal Division. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Washington, D.C.: 2009).

networks and other third parties, and trade associations and other experts and researchers. For example, FTC said that operating systems should provide disclosures at the point in time when consumers access location-based services and obtain their affirmative express consent before allowing applications to access sensitive content like location data.

Federal Law Addressing Location Data Privacy Is Not Comprehensive

Currently, no comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies; rather, various federal laws pertain to the privacy of consumers' data:[15]

- The Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce and authorizes FTC enforcement action.[16] This authority allows FTC to take remedial action against a company that engages in a practice that FTC has found is unfair or deceives customers. For example, FTC could take action against a company if it found the company was not adhering to the practices to protect a consumer's personal information that the company claimed to abide by in its privacy policy.
- The Electronic Communications Privacy Act of 1986 (ECPA), as amended, sets out requirements under which the government and providers of electronic communications can access and share the content of a consumer's electronic communications.[17] ECPA also prohibits providers of electronic communications from voluntarily disclosing customer records to government entities, with certain exceptions, but companies may disclose such records to a person other than government entities. The act does not specifically address whether location data are considered content or part of consumers' records. Some privacy groups have stated that ECPA should specifically address the protection of location data. The act also

[15]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[16]An act or practice is unfair if the injury it causes or is likely to cause to consumers is: (1) substantial; (2) not outweighed by countervailing benefits to consumers or to competition; and (3) not reasonably avoidable by consumers themselves. 15 U.S.C. § 45. A representation, omission, or practice is deceptive if: (1) it is likely to mislead consumers acting reasonably under the circumstances; and (2) it is material, that is, likely to affect consumers' conduct or decisions with respect to the product at issue. See e.g., Federal Trade Commission v. Patriot Alcohol Testers, Inc., 798 F. Supp. 851 (D. Mass. 1992).

[17]See, e.g., 18 U.S.C. §§ 2702, 2511.

provides legal procedures for obtaining court orders to acquire information relevant to a law enforcement inquiry.

- The Communications Act of 1934 (Communications Act), as amended, imposes a duty on telecommunications carriers to secure information and imposes particular requirements for protecting information identified as customer proprietary network information (CPNI), including the location of customers when they make calls.[18]The Communications Act requires that companies obtain express authorization from consumers before they access or disclose call location information, subject to certain exceptions.[19] Carriers must also comply with FCC rules implementing the E911 requirements of the Wireless Communications and Public Safety Act of 1999,[20] including providing location information to emergency responders when mobile phone consumers dial 911.[21]

We have previously concluded that the current privacy framework warrants reconsideration in relation to a number of issues. In our 2013 report on consumer data collected and shared by information resellers[22], we found that changes in technology and the marketplace have vastly increased the amount and nature of personal information, including location data that are collected, used, and shared. We reported that while some stakeholders' views differed, the current statutory framework does not fully address these changes. Moreover, we reported that while current laws protect privacy interests in specific sectors and for specific uses, consumers have little control over how their information is collected, used, and shared with third parties. This includes consumers' ability to access, correct, and control their personal information used for marketing, such as location data, and privacy controls related to the use of new technologies and applications, such as mobile and in-car navigation devices. In 2012,

[18]CPNI includes information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service as well as information contained in the bills pertaining to telephone service. As the Communications Act requirements for CPNI apply only to carriers, they would not apply to other types of companies that collect and use mobile phone location data, such as application developers. 47 U.S.C. § 222(f), (h).

[19]47 U.S.C. §222(f)(1).

[20]Pub. L. No. 106-81 (Oct. 26, 1999).

[21]47 C.F.R. § 20.18.

[22]GAO-13-663.

FTC and NTIA called on Congress to pass data privacy legislation that would provide a minimum level of protection for consumer data, including location data. Some Members of Congress have introduced legislative proposals that address the privacy of consumers' location data.[23]

Chairman Franken, Ranking Member Flake, and Members of the Subcommittee, this concludes my prepared remarks. I am happy to respond to any questions that you or other Members of the Subcommittee may have at this time.

GAO Contact and Staff Acknowledgement

For questions about this statement, please contact Mark L. Goldstein, Director, Physical Infrastructure Issues, at (202) 512-2834 or goldsteinm@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this statement include Andrew Von Ah (Assistant Director), Michael Clements, Roshni Davé, Colin Fallon, Andrew Huddleston, Lori Rectanus, and Crystal Wesco.

[23]See e.g., S. 2171, 113th Cong. (2014); S. 639, 113th Cong. (2013); H.R. 1312, 113th Cong. (2013).

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

PREPARED STATEMENT OF BRIAN HILL

The Testimony of
Detective Brian Hill
Criminal Investigations Division
Anoka County Sheriff's Office

For the Hearing of the Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
United States Senate
Location Privacy Protection Act of 2014

June 4, 2014

Introduction

Chairman Franken, Ranking Member Flake, and distinguished Members of the Subcommittee, my name is Brian Hill and I thank you for the opportunity to appear before the Subcommittee to testify about law enforcement's support of the Location Privacy Protection Act of 2014.

Background and Expertise in Cyberstalking Investigations

I am a Detective with the Criminal Investigations Division (CID) of the Anoka County Sheriff's Office in Minnesota. I have been working in my role as a Detective with the Criminal Investigations Division since 2008 and am responsible for the investigation of domestic violence and criminal sexual conduct cases, suspicious deaths, homicides, missing persons, and fatal motor vehicle accidents occurring in our county. We serve the fourth most populous county in Minnesota and have developed an extensive digital forensics lab which is one-of-its-kind in our state.

I am a Computer/Mobile Device Forensic Examiner/Investigator trained by the Minnesota Bureau of Criminal Apprehension, the Federal Bureau of Investigation, and the Secret Service. I have a Cell Phone Technology and Forensic Data Recovery Certification (CTF), Advanced Cellular Technology & Smartphone Forensics Certification (+SMART), Access Data Bootcamp Certification (FTK), Access Data Certified Examiner (ACE) and Access Data Mobile Examiner (AME). I am a member of the High Technology Crime Investigators Association (HTCIA). I also serve on the Board of Directors of the Minnesota Chapter of HTCIA as the 1st Vice President. Additionally, I served in the Air Force Reserves

from 1997 to 2006 in the 96th Airlift Squadron and was deployed from March 2003 to March 2005 for the wars in Iraq and Afghanistan.

GPS "Stalking Apps": Widespread, Serious Safety Threat

The use of "stalking apps" to perpetrate cyberstalking poses serious safety risks to victims of domestic violence.

I worked with a victim a couple years ago where she suspected that her estranged boyfriend must have put some type of spyware on her phone. She stated that he would know things about private conversations that she had over the phone and in text messages. Also he would show up randomly at locations where she was. I did an exam of her phone and was unable to get a full data extraction off of the phone and unable to determine if there was any spyware. Later, she brought in her computer for me to look at and I was able to find that the program FlexiSPY was accessed on the computer. I was then able to show that the program was installed on her phone and was able to work with her to get a new phone and set up new email accounts on a safe computer.

After stealth cyberstalking has begun, regaining safety is a difficult and expensive process for victims. On top of the trauma of surviving domestic abuse, victims are economically and socially impacted. They often must buy new phones, computers, and other technological equipment to be rid of the stealth stalking apps – although there are never any guarantees. Additionally, as we all become more accustomed to using our phones to work, bank, text, email, access social media, search the internet, and pay bills, stealth cyberstalking not only financially impacts victims, but can serve as a tool to isolate victims from all of the functions and social connections their phones provide – including isolating them from being able to reach out to domestic violence advocates or law enforcement. If victims want to be rid of stealth stalking apps they must create new email accounts and change all passwords and security questions – although, again, there are never any guarantees. It is terrifying for victims to know that they will never really know if the stealth stalking apps are gone or if they will reappear after being removed. This means victims' privacy and peace of mind continue to be violated, often long after they have bought new phones or changed their passwords.

These harrowing victim experiences are more and more commonplace through the proliferation of stalking apps. As I have been performing digital forensic examinations since 2008, I continue to discover new apps, especially as they become cheaper and more readily available. For instance, our office is

currently investigating an attempted murder in the context of domestic violence. When we examined the victim's phone, we discovered Ti-spy, running in stealth mode on her mobile device. Ti-Spy is an internet company that advertises itself as parental monitoring software. The software costs just $7 per month and can be installed on any Android smartphone. The software advertises that it can track text messages, calls, GPS locations, and basically access any data contained on the phone that the software has been installed on.

As in the case of discovering Ti-spy, I typically become engaged in a forensic investigation after victims, their domestic violence advocates or law enforcement detect the unsettling signs of digital wrongdoing. They notice a pattern of the abuser knowing all kinds of information about where a victim is and what she is doing, when there is no way the abuser should know those things. In the last 3 years, the mobile forensic examinations I conduct have increased exponentially – by 220%[1] – and I only investigate felony level domestic violence crimes in just one out of 87 counties in Minnesota. We currently average 30 forensic exams per month, again only on felony level cases.

Lack of Resources & Awareness Undercut Law Enforcement Response to Cyberstalking

While my department deals with only felony cases, stalking apps are frequently used in misdemeanor and gross misdemeanor domestic violence cases. Most local law enforcement, however, do not have the resources, staffing time, training, or forensic equipment to examine mobile devices for GPS stalking apps operating in stealth mode.

Investigating cyberstalking is labor intensive and requires expensive specialized equipment. Anoka County is fortunate to have eight tools we use for forensic examinations.[2] Anoka County also has dedicated staff to perform the investigations.

Other law enforcement agencies may have one exam tool, at best, and little to no dedicated staff time to conduct the forensic examinations. If agencies rely on just one tool or rely only on what is visible on a victim's phone, they are potentially receiving just 5% of the data off a phone and thus, losing a large amount of potential evidence that can be helpful in keeping victims safe. Because of Anoka County's resources, we frequently have detectives and domestic advocates from other counties requesting that we

[1] Anoka County Mobile Phone Exams as reported by the Anoka County Sheriff's Office: 2011 – 171 exams; 2012 – 240 exams; 2013 – 377 exams; 2014 YTD through April – 119 exams.
[2] Katana – Lantern; Cellebrite Ultimate – UFED TOUCH; Cellebrite - Classic; Susteen – Secure View; Microsystemation – XRY; Oxygen Forensics Suite; Accessdata – MPE Plus; Paraben – Device Seizure.

perform exams for cases in other jurisdictions. In fact, federal agencies have also asked us to perform forensic exams for them.

This resource problem is so widespread that in a recent survey conducted by the Minnesota Coalition for Battered Women in conjunction with Minnesota Court Administration, advocates indicated that cyberstalking was the number one priority for law enforcement training in the protective order context. Because technology is frequently used to stalk victims and violate protective orders, law enforcement's awareness and capacity to respond to victim reports is key to safety and accountability.

To address the need for training on cyberstalking, I have worked closely with the Minnesota Coalition for Battered Women, and its 80+ member programs, in developing and conducting several trainings and curricula. Since 2009, I have trained over 3,000 domestic and sexual assault advocates, prosecutors, judges, general crime advocates, corrections officers, law enforcement, and community members in Minnesota and around the country. The trainings have focused on (1) the use of technology in intimate partner stalking; (2) securing and gathering evidence in technology assisted crimes; and (3) the use of technology in violations of protective orders.

Our efforts have borne fruit, but strained resources and a lack of awareness continue to undercut law enforcement's ability to recognize and respond to domestic violence victims' increasing reports of cyberstalking. This erodes victim trust in the criminal justice system. A common abuser tactic in domestic violence is to convince the victim she is crazy. There are few things that will drive you crazy more than a victim reporting that she believes he is using stealth stalking apps only to be told: we don't believe you or we don't have the resources to examine your phone. When law enforcement can't effectively identify and respond to cyberstalking reports, victims stop reporting the crimes and abusers win.

A Meaningful Solution to Cyberstalking: The Location Privacy Protection Act of 2014

The Location Privacy Protection Act of 2014 is a major step in addressing the proliferation of stalking apps in the context of domestic violence, by banning the development, operation, and sale of GPS stalking apps. This is important because in order to combat this issue we need to go after the companies that make and market these applications. It comes down to economics, and if we make it unprofitable for the companies to make these programs, then we can help ensure that abusers don't have access to them.

Secondly, the bill supports victim safety by requiring that stalking apps running in stealth mode alert the user and request permission to run. It requires that *all* apps get permission to collect or share location information, making sure that a stalking app can't disguise itself as an employee, or family tracking app – or simply as a flashlight app.

In my opinion, the most important part of the Location Privacy Protection Act of 2014 is that apps will be required to notify the user a second time – 24 hours or seven days after installation – about the tracking implications. This allows for a victim to be notified when the perpetrator doesn't have access to the phone. If this notice only applied to stalking applications, they would just simply change the name of the app or market it in a different way. Just like in human trafficking when Craigslist no longer allowed certain ads, the company backpages.com emerged and began to offer those ads. This Act would address such evasion of the law.

Finally, the Act will bring national public awareness to this serious and widespread issue by requiring that the federal government gather more information about GPS stalking, facilitate reporting of GPS stalking, and prioritize training grants for law enforcement.

I urge you to support the Location Privacy Protection Act of 2014.

Thank you again to the committee for reviewing my testimony and for your support of law enforcement's efforts to keep domestic violence victims and our communities safe.

PREPARED STATEMENT OF LUIGI MASTRIA

BEFORE THE

U.S. SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

HEARING ON

THE LOCATION PRIVACY PROTECTION ACT OF 2014

JUNE 4, 2014

TESTIMONY OF

LUIGI MASTRIA, CIPP, CISSP

EXECUTIVE DIRECTOR

DIGITAL ADVERTISING ALLIANCE

Chairman Franken, Ranking Member Flake, and Members of the Subcommittee, good afternoon and thank you for the opportunity to speak at this important hearing.

My name is Lou Mastria. I am Executive Director of the Digital Advertising Alliance ("DAA") and I am pleased to report to the Committee on industry's success in providing consumers with transparency and choice online with respect to data collection and use and the substantial progress of our Self-Regulatory Program in extending these consumer friendly standards to mobile environments.

The DAA is a non-profit organization founded by the leading advertising and marketing trade associations including the Association of National Advertisers ("ANA"), the American Association of Advertising Agencies ("4As"), the Direct Marketing Association ("DMA"), the Interactive Advertising Bureau ("IAB"), the American Advertising Federation ("AAF"), and the Network Advertising Initiative ("NAI"), in consultation with the Council of Better Business Bureaus ("CBBB"). These organizations came together in 2008 to start developing the Self-Regulatory Principles for Online Behavioral Advertising, which were extended in 2011 beyond advertising to cover the collection and use of Multi-Site Data across non-Affiliate sites over time, and then again extended in July 2013 to provide guidance for data collection in mobile environments. The DAA was formed to administer and promote these responsible and comprehensive Self-Regulatory Principles for online data collection and use.

We believe the DAA is a model example of how interested stakeholders can collaborate across the ecosystem to provide meaningful and pragmatic solutions to complex privacy issues, especially in areas as highly dynamic and evolving as mobile advertising. In my testimony, I will describe the benefits of digital advertising and self-regulation and how the industry, through

the DAA, provides consumer-friendly privacy standards in a way that also ensures the continued vibrancy of the Internet and our nation's place as the global leader in the data-driven economy.

I. Benefits of Digital Advertising

The Internet is a tremendous engine of economic growth. It has become the focus and a symbol of the United States' famed innovation, ingenuity, inventiveness, and entrepreneurial spirit, as well as the private-sector venture funding and the advertising support that follows. Simply put: the Internet economy and the interactive advertising industry create jobs. A 2012 study found that the Internet economy supports the employment of more than five million Americans, contributing an estimated $530 billion, or approximately 3%, to our country's GDP.[1] There is Internet employment in every single state.[2] Another recent study, commissioned by DMA's Data-Driven Marketing Institute ("DDMI") and conducted independently by Professors John Deighton of Harvard Business School and Peter Johnson of Columbia University, and entitled "The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy" ("Value of Data"), quantifies the value data has to our economy. The Value of Data study found that the Data-Driven Market Economy ("DDME") added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012 alone. The study also found that an additional 1,038,000 jobs owe part of their existence to these DDME jobs. The study estimated that 70% of the value of the DDME – $110 billion in revenue and 475,000 jobs nationwide – depends on the ability of firms to share data across the DDME.

Advertising fuels this powerful Internet economic engine. The support provided by online advertising is substantial. In 2013, Internet advertising revenues reached a new high of

---

[1] Professor John Deighton, Harvard Business School, *Economic Value of the Advertising-Supported Internet Ecosystem*, at 81 (September 2012), available at http://www.iab.net/media/file/iab_Report_September-24-2012_4clr_v1.pdf (last visited May 12, 2014).
[2] *Id.* at 66.

$43 billion, an impressive 17% higher than 2012's full-year number.[3] Innovation and growth in mobile has helped lead the way in the ad-supported ecosystem's positive impact on the American and global economies. Mobile advertising in the United States totaled $7.1 billion during FY 2013, a 110% increase from the prior year total of $3.4 billion, with strong growth taking place across formats, including search, display, and messaging. Mobile now accounts for 17% of total digital ad revenue.

Because of advertising, consumers can access a wealth of online and mobile resources at low or no cost. Revenue from online and mobile advertising enables e-commerce and subsidizes the cost of content and services that consumers value, such as digital newspapers, blogs, social networking sites, mobile applications, email, and phone services. These advertising-supported resources have transformed our daily lives.

Interest-based advertising is an essential form of online and mobile advertising. Consumers are likely to find interest-based advertisements more relevant to them, and advertisers are more likely to attract consumers that want their products and services. Interest-based advertising is especially vital for small businesses because it is efficient. Smaller advertisers can stretch their marketing budgets to reach consumers who may be interested in their offerings. Smaller website publishers that cannot afford to employ sales personnel to sell their advertising space, and may be less attractive to large brand-name advertising campaigns, can increase their revenue by featuring advertising that is more relevant to their users. In turn, advertising-supported resources help other small businesses to grow. Small businesses can use free or low-cost online tools, such as long-distance calling, and networking services, to help them run their companies.

---

[3] Interactive Advertising Bureau 2013 Internet Advertising Report (April 2014) (reporting results of PricewaterhouseCoopers study), available at http://www.iab.net/AdRevenueReport (last visited on May 12, 2014).

II. Benefits of Industry Self-Regulation

The DAA's commitment to self-regulation has put us at the forefront of new consumer protection initiatives. The DAA believes that self-regulation is the appropriate approach for addressing the interplay of privacy and online and mobile advertising practices. We believe that our approach has been successful in addressing consumer concerns while ensuring that the U.S. Internet economy remains vibrant. Self-regulation provides industry with a nimble way of responding to new challenges presented by the evolving Internet ecosystem, which is particularly important for nascent markets like mobile. For our information-driven economy to thrive and continue as an engine of job creation, self-regulation led by industry codes of conduct is the ideal way to balance privacy and innovation.

Based on the DAA's commitment to advancing industry self-regulation, we are concerned about some of the proposals put forward by the Administration and the Federal Trade Commission in their respective consumer data privacy frameworks.[4] In particular, both the Administration and the Federal Trade Commission have called for comprehensive legislation in the area of consumer data privacy. The DAA does not believe that such new legislation is needed at this time. The DAA is concerned that laws and regulations are inflexible and can quickly become outdated in the face of extraordinarily rapidly-evolving technologies. When this occurs, legislation thwarts innovation and hinders economic growth.

Laws and regulations can also serve as a disincentive to the marketplace to innovate in the area of privacy. Companies are increasingly offering consumers new privacy features and tools such as sophisticated preference managers, persistent opt outs, universal choice mechanisms, and shortened data retention policies. These developments demonstrate that

[4] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012); Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).

companies are responsive to consumers and that companies are focusing on privacy as a means to distinguish themselves in the marketplace. The DAA believes that this impressive competition and innovation should be encouraged. New laws or rules could impede future developments or discourage companies from continuing to compete over privacy features. We believe that the DAA program, which industry has already invested millions of dollars to develop, is clearly one of the most successful and fastest-developing self-regulatory systems in U.S. history and should be allowed to continue to flourish without unneeded governmental intervention or legislation at this time.

III. The DAA

As the DAA was convened, its goal was to provide greater transparency and control to consumers with respect to their Web viewing data while preserving these incredible benefits to consumers and our economy. Since 2008, the DAA has worked with a broad set of stakeholders with significant input from businesses, consumers, and policy makers to develop a program governing the responsible collection and use of Web viewing data. This work led to the development of the groundbreaking *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles"), released in 2009, and the *Self-Regulatory Principles for Multi-Site Data* ("MSD Principles"), released in 2011. DAA evolved again to provide guidance with release of the *Application of Self-Regulatory Principles to Environments* ("Mobile Guidance") in 2013.

The DAA approach provides consumers choice with respect to collection and use of their Internet viewing data while preserving the ability of companies to responsibly deliver services and continue innovating. This approach allows consumers to enjoy the incredibly diverse range of Web sites by preserving the responsible data flows that support these offerings and that fuel

our nation's economy. The DAA approach also provides heightened safeguards for the collection and use of sensitive data.

The successful approach taken by the DAA led to an event in February 2012 at the White House where the Chairman of the Federal Trade Commission ("FTC"), the Secretary of Commerce, and White House officials publicly praised the DAA's cross-industry initiative. The White House recognized our Self-Regulatory Program as "an example of the value of industry leadership as a critical part of privacy protection going forward."[5] Since the White House event, the DAA's further work in releasing the MSD Principles and Mobile Guidance has garnered additional praise, including from FTC Commissioner Ohlhausen who has stated that the DAA "is one of the great success stories in the [privacy] space."[6]

The DAA Principles apply broadly to the diverse set of actors that work interdependently to deliver relevant advertising intended to enrich the consumer digital experience, and to foster consumer-friendly privacy standards that are to be applied throughout the ecosystem. The Principles were developed over a year-long period in which broad consensus was reached among the key constituencies of the Internet community. These Principles call for (1) enhanced notice outside of the privacy policy so that consumers can be made aware of the companies they interact with while using the Internet, (2) the provision of choice mechanisms, (3) education, and (4) strong enforcement mechanisms. Together, these Principles increase consumers' trust and confidence in how information is gathered online and in mobile environments and how it is used to deliver advertisements based on their interests. The Principles also restrict the collection of

[5] Speech by Danny Weitzner, *We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age* (February 23, 2012), available at http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age (last visited June 3, 2014).
[6] Katy Bachman, *FTC's Ohlhausen Favors Privacy Self-Regulation* (June 3, 2013), available at http://www.adweek.com/news/technology/ftcs-ohlhausen-favors-privacy-self-regulation-150036 (last visited June 3, 2014).

sensitive data and the use of all data for specified eligibility purposes including employment; credit; healthcare treatment; and insurance and underwriting and pricing. These same safeguards are also part of the Mobile Guidance.

A. Consumer Disclosure through the DAA Icon

The DAA program has developed a universal icon to give consumers transparency and control with respect to interest-based ads. The icon provides consumers with notice that information about their online interests is being gathered to customize the Web ads they see. Clicking the icon also takes consumers to a centralized choice tool that enables consumers to opt out of this type of advertising by participating companies.

The icon is served globally more than *one trillion times each month* on or next to Internet display ads, websites, and other digital properties and tools covered by the program. This achievement represents an unprecedented level of industry cooperation and adoption. The DAA is building products to provide the same level of transparency in the mobile environment.

B. Consumer Control

At DAA's *www.aboutads.info* website and accessible from the companion *www.YourAdChoices.com* educational website, the DAA program makes available a choice mechanism that unites the opt-out mechanisms provided by more than 115 different third-party ad technology companies participating in the program. The choice mechanism offers consumers a "one-click" option to request opt outs from all participants or allows a user to make choices about specific companies. Consumers are directed to aboutads.info not only from DAA icon-based disclosures on or around ads, but from other forms of website disclosure. In 2012, the DAA also introduced a suite of browser plug-ins to help ensure the persistency of these choices.

Since program launch, there have been more than 30 million unique visitors to the DAA program Web sites. *Over three million unique users* have exercised choice using the integrated opt-out mechanism provided at AboutAds.info. Many users visit DAA program Web sites, learn about their choices, and ultimately choose not to opt out. This shows that once consumers understand how online advertising works, many prefer to receive relevant ads over irrelevant ads. Research supports this proposition. A recent poll of U.S. consumers shows that 68 percent of Americans prefer to get at least some Internet ads directed at their interests and 40 percent of Americans prefer to get all their ads directed to their interests.[7]

C. Consumer Education

The DAA is also committed to consumer education. The DAA launched a dedicated educational site at *www.YourAdChoices.com* to provide easy-to-understand messaging and informative videos explaining the choices available to consumers, the meaning of the DAA icon, and the benefits they derive from online advertising. Companies participating in the DAA program have donated voluntarily more than four billion impressions to support an educational campaign for *www.YourAdChoices.com*. More than *15 million unique users* have visited this site. This site also provides access to the DAA's user choice mechanism. The combination of the educational campaign and the ubiquitous availability of the DAA icon have significantly increased consumer usage of the DAA program tools.

D. Accountability

For the past 40 years, the advertising industry has distinguished itself through its self-regulatory systems for independent oversight of compliance and public reporting of enforcement actions. In keeping with this tradition, a key feature of the DAA Self-Regulatory Program is

[7] Interactive Survey of U.S. Adults commissioned by the DAA (April 2013), *available at* http://www.aboutads.info/DAA-Zogby-Poll.

independent accountability. All of the DAA's Self-Regulatory Principles are backed by the robust enforcement programs administered by the Council of Better Business Bureaus ("CBBB") under the policy guidance of the Advertising Self-Regulatory Council (ASRC), and by the DMA under its Guidelines for Ethical Business Practice. A more detailed description of how these programs work is included in Appendix I.

E. Application of Self-Regulatory Principles to the Mobile Environment

The DAA Self-Regulatory Program has adapted over time and we expect this evolution to continue with changes in the marketplace driven by technological advancements and evolving consumer preferences. In July 2013, the DAA issued new implementation guidance addressing certain operations across a variety of channels including mobile (the "Mobile Guidance"). This guidance brings the same consumer privacy safeguards operating in the online environment to mobile web and mobile applications. The Mobile Guidance explains how the Self-Regulatory Principles apply to certain data practices that may occur on mobile or other devices.

Stakeholders representing all major elements of the mobile ecosystem participated in the development of this guidance. The guidance describes how the Self-Regulatory Principles apply to the mobile web environment and to the application environment, including to what the DAA calls "Cross-App" data – data collected from a device across non-Affiliated applications over time. In April 2014, the DAA issued detailed guidance for displaying the DAA icon in mobile environments. The DAA has now turned its work with DAA stakeholders to develop and implement a companion transparency and choice mechanism for Cross-App Data. In the coming months, the DAA will release a new choice tool that will offer consumers an unprecedented level of control over data collection across applications on a device. DAA expects this choice mechanism to be operational in 2014. Once available, the DAA will announce to covered

companies that this guidance is effective and enforceable. Any entity engaged in the collection and use of Cross-App Data after the effective date established by the DAA will be subject to the DAA accountability mechanisms for engaging in practices that do not adhere to the Self-Regulatory Principles.

F. Precise Location Data

The DAA program requires companies to adhere to stringent requirements for location data gathered in mobile environments. These requirements include consent for collection and the provision of enhanced transparency.

The Mobile Guidance squarely addresses control over Precise Location Data – data obtained from a device about the physical location of that device that is sufficiently precise to locate a specific individual or device – requiring entities collecting such data to obtain consumers' consent, or obtain reasonable assurances that the app developer or owner has obtained consent to the third party's data collection, use, and transfer. In addition, the DAA program requires companies to provide an easy-to-use tool to withdraw consent at any time.

The Mobile Guidance further calls for entities to provide clear, meaningful, and prominent notice regarding their collection and use of Precise Location Data. An app provider – also known as a First Party – must include in the notice the fact that Precise Location Data is transferred to or collected by a Third Party and instructions for accessing and using a consent tool. Third Parties must include these same disclosures, as well as the uses of Precise Location Data, such as whether it will be transferred to a non-Affiliate, and must display the notice on their web sites or the applications from or through which they collect Precise Location Data.

First Parties are called upon to provide enhanced notice – outside of the privacy policy – of Third Parties' collection and use of Precise Location Data from or through a First Party's

application. This enhanced notice must be made (a) as part of the downloading process; (b) at the time that the app is first opened; or (c) at the time the data is collected. First Parties must also provide a link to their disclosures through the enhanced notice process as well as in the application's settings or privacy policy.

III. Conclusion

The DAA has championed consumer control that both accommodates consumers' privacy preferences and supports companies' ability to continue innovating and responsibly delivering the products and services desired by consumers. We appreciate the opportunity to be here today.

I am pleased to answer any questions that you may have.

* * *

APPENDIX I: ACCOUNTABILITY PROGRAMS

The CBBB Accountability Program builds on the successful track records of the other ASRC programs: the National Advertising Division, operating since 1971; the Children's Advertising Review Unit, operating since 1974; and the Electronic Retailing Self-Regulation Program, operating since 2004. These programs feature independent monitoring; public reporting of decisions; and referral to government agencies, often to the FTC, of any uncorrected non-compliance. They have extremely high voluntary compliance rates. In fact, over 90 percent of companies voluntarily adopt the recommendations of these programs. Those companies that fail to comply or refuse to participate in the self-regulatory enforcement process are referred publicly to the appropriate government agency for further review.

The CBBB administers its Interest-Based Advertising Accountability Program under the ASRC self-regulatory policy guidance and procedures. Because of the highly complex, technical and interdependent nature of interest-based advertising, the Accountability Program receives a weekly privacy dashboard report based on independent data about more than 250 companies' compliance with various requirements of the Principles. The Accountability Program's technical staff analyzes these data and independently performs further research to determine whether there may be a violation of the Principles warranting formal inquiry. Like other ASRC programs administered by the CBBB, the CBBB Accountability Program also finds potential cases through its own staff monitoring and investigation, by analysis of consumer complaints and reviews of news stories and technical reports from academics and advocacy groups. Where there is a potential compliance issue, the CBBB initiates formal inquiries and works to ensure the company understands the Principles and voluntarily implements the requirements of the Principles. At the end of the process, the CBBB Accountability Program issues a public decision, which details the

nature of the inquiry, the Accountability Program's conclusions, any recommendations for correction, and includes a statement from the company in question regarding its implementation of the recommendations. A press release is also issued.

The CBBB's Accountability Program has brought 33 cases since November 2011. The CBBB Accountability Program has focused its inquiries on the key concepts of transparency and choice under the DAA's Self-Regulatory Principles. In its initial round of cases, the Accountability Program investigated whether companies were correctly and reliably providing consumers with an effective choice mechanism. Cases involved defective links to opt-out mechanisms and transparency that was deficient or otherwise lacking.

The DMA's enforcement program likewise builds on a long history of proactive and robust self-regulatory oversight. The DMA's longstanding Guidelines for Ethical Business Practice ("Guidelines") set out comprehensive standards for marketing practices, which all DMA members must follow as a condition of membership. The DAA Self-Regulatory Principles are incorporated into these Guidelines.

The DMA's Committee on Ethical Business Practice examines practices that may violate DMA Guidelines. To date, the DMA Guidelines have been applied to hundreds of marketing cases on a variety of issues such as deception, unfair business practices, personal information protection, and online behavioral advertising. In order to educate marketing professionals on acceptable marketing practices, a case report is regularly issued which summarizes questioned direct marketing promotions and how cases were administered. The report also is used to educate regulators and others interested in consumer protection issues about the DMA Guidelines and how they are implemented.

The Committee on Ethical Business Practice works with both member and non-member companies to gain voluntary cooperation in adhering to the guidelines and to increase good business practices for direct marketers. The DMA Corporate Responsibility team and Ethics Committee receive matters for review in a number of ways: from consumers; member companies; non-members; or, sometimes, consumer protection agencies. Complaints are reviewed against the Guidelines and Committee members determine how to proceed. If a potential violation is found to exist, the company will be contacted and advised on how it can come into full compliance.

Most companies work with the Committee to cease or change the questioned practice. However, if a member company does not cooperate and the Committee believes there are ongoing Guidelines violations, the Committee can recommend that action be taken by the Board of Directors and can make case results public. Board action could include censure, suspension or expulsion from membership, and the Board may also make its actions public. If a non-member or a member company does not cooperate and the Committee believes violations of law may also have occurred, the case is referred to federal and/or state law enforcement authorities for review.

The CBBB and DMA programs demonstrate the success of self-regulation and its many benefits, including the ability for the regulatory apparatus to evolve to meet new challenges. Importantly, accountability under the Principles applies to all members of the advertising ecosystem, not merely "members" of the various organizations.

PREPARED STATEMENT OF SALLY GREENBERG

Testimony of

Sally Greenberg

Executive Director

National Consumers League

Hearing on S. 2171

The Location Privacy Protection Act of 2014

Before the

United States Senate

Committee on the Judiciary

Subcommittee on Privacy, Technology and the Law

June 4, 2014

Introduction

Good afternoon Chairman Franken, Ranking Member Flake and members of the subcommittee. My name is Sally Greenberg and I am the Executive Director of the National Consumers League (NCL).[1] Founded in 1899, NCL is the nation's pioneering consumer organization. Our non-profit mission is to advocate on behalf of consumers and workers in the United States and abroad. I appreciate this opportunity to appear before the subcommittee to speak in support of S. 2171 and I applaud you for considering this critically important consumer privacy protection bill.

The Right to Privacy is a Bedrock Principle of American Democracy

Supreme Court Justice Louis Brandeis – who served as NCL's general counsel – noted in a landmark 1928 decision that the right to privacy is "the most comprehensive of rights, and the right most valued by civilized men."[2] We could not agree more. NCL believes that privacy is a cornerstone of consumer protection and a fundamental human right.

According to a *Consumer Reports* poll from 2012, most consumers are "very concerned" about Internet firms selling information about them without their

---

[1] The National Consumers League, founded in 1899, is America's pioneer consumer organization. Our non-profit mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. For more information, visit www.nclnet.org.

[2] *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, L., dissenting). Online: http://www.law.cornell.edu/supremecourt/text/277/438#writing-USSC_CR_0277_0438_ZD

permission. The poll found that 71% of consumers were very concerned about online data collection, while 65% were worried about the way smartphone apps could access their personal contacts, photos, location and other data without their permission.[3] A *Los Angeles Times* poll showed similar results; 82% of Californians were very or somewhat concerned about Internet and smartphone firms collecting their information.[4]

As new technologies, products, and services are introduced into the marketplace, their ability to gather information and share data broadly without sufficient privacy rules and protections in place is of great concern. This is why NCL supports S. 2171, the Location Privacy Protection Act of 2014, which will put in place a privacy protection regime that is adapted to today's mobile data ecosystem.

This bill proposes a modest approach to protecting consumer privacy and includes exceptions for parental rights, national security, law enforcement or other discrete circumstances. We support affirmative consumer consent prior to the collection of location information and disclosure about the purpose of such collection and the uses of that information. Consumers must have control over whether and how their location information is used, particularly if it is to be used for purposes other than those for which it was originally obtained. We also believe

---

[3] Sarno, David. "Consumer Reports, Times polls find broad data privacy concerns," *The Los Angeles Times*. April 3, 2012. Online: http://articles.latimes.com/2012/apr/03/business/la-fi-tn-consumer-reports-privacy-20120403

[4] *Id.*

that consumers should have a private right of action to obtain redress when breaches of their privacy occur.

Privacy Breaches Threaten Trust in Location-Based Services

The ubiquity of smartphones, tablets and other mobile devices has dramatically changed the way consumers interact with the digital world. There is no question that consumers love the convenience and functionality of the array of apps and other mobile technologies available to them today. Thanks to the widespread use of location data, enabled by technologies such as GPS, consumers can now navigate to their favorite coffee shops, discover the closest sushi restaurant and be more easily located by emergency response providers. This technology has clearly provided immense consumer benefits.

The wide adoption of location-aware devices has also spawned a growing industry. In May 2011, only 35% of American adults owned smartphones. Today, 58% of adults own them.[5] Marketers are increasingly cashing in on the treasure trove of location data that the proliferation of such devices has created. According to one study, the $3.9 billion currently spent on "geo-targeted" mobile advertising tailored to a user's precise location is likely to grow to $9.1 billion by 2017.[6]

---

[5] Smith, Aaron. *Smartphone Ownership 2013.* June 5, 2013. Online: http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/

[6] BIA/Kelsey. "BIA/Kelsey Forecasts U.S. Mobile Local Ad Revenue to Reach $9.1 Billion in 2017," Press Release. April 4, 2013. Online: http://www.biakelsey.com/Company/Press-Releases/130404-U.S.-Mobile-Local-Ad-Revenues-to-Reach-$9.1-Billion-in-2017.asp

As the collection and use of location data has become an integral part of the mobile ecosystem, so too has consumer concern over the use – and misuse – of these data. Consumers place special value on their location data. They are less comfortable sharing this information with people they don't know and they want more control over it.[7] This should not be surprising. Unlike location data gained from a non-mobile device, such as a desktop computer, data from mobile devices is inherently personal and can be used to learn and possibly disclose information that in many cases consumers would rather be kept private. Supreme Court Justice Sotomayor underscored the sensitivity of location data in her concurring opinion in *U.S. v. Jones* when, quoting from an earlier New York case, she wrote:

> *"Disclosed in [GPS] data... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal*

[7] See, e.g., Janice Y. Tsai, Patrick Kelley, Paul Drielsma, Lorrie Cranor, Jason Hong, Norman Sadeh, Who's viewed you?: the impact of feedback in a mobile location-sharing application, Conference on Human Factors in Computing Systems: Proceedings of the 27th international conference on human factors in computing systems (2009), http://www.cs.cmu.edu/~sadeh/Publications/Privacy/CHI2009.pdf; Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge, Location Disclosure to Social Relations: Why, When, & What People Want to Share, CHI '05: Proceedings of the SIGCHI conference on human factors in computing systems (2005), www.placelab.org/publications/pubs/chi05-locDisSocRel-proceedings.pdf.

defense attorney, the by-the- hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[8]

While reputable businesses may recognize and respect the sensitivity of location data, the rules that govern use of these data are largely voluntary. In addition, there are significant loopholes and confusion regarding the applicability of current laws to sensitive location data. We need only look to the recent past to find incidences where businesses have failed to follow industry best practices. For example:

- In August 2011, it was reported that Windows 7 smartphones were sending their users' location to Microsoft when the camera app was on. This data sharing happened even when users denied consent to do so.[9]

- In December 2013, the makers of the Brightest Flashlight Android app settled a FTC enforcement action alleging that, contrary to their privacy

[8] UNITED STATES v. JONES () 615 F. 3d 544. Online: http://www.law.cornell.edu/supremecourt/text/10-1259

[9] Levine, Dan. "Lawsuit says Microsoft tracks customers without consent," *Reuters*. August 31, 2011. Online: http://www.reuters.com/article/2011/08/31/us-microsoft-lawsuit-idUSTRE77U6BT20110831

policy, the makers of the app disclosed users' precise location and unique device identifier to third parties, including advertising networks.[10]

- We learned in February of this year that the dating app Tinder allowed any user of the app to identify another user's location to within 100 feet, not the nearest mile as the app promised. This was the second time in less than a year that this app was found to be broadcasting sensitive location data.[11]

- Just last month, the FTC settled charges against Snapchat, Inc. – makers of a popular photo-sharing app – that the company collected and transmitted location of information from users of its Android app despite claims in its privacy policy that it did not track this information.[12]

These are just a few recent examples of companies failing adhere to their own stated privacy policies and play fair with consumers' location data.

---

[10] Federal Trade Commission. "Android Flashlight App Developer Settles FTC Charges It Deceived Consumers," Press Release. December 5, 2013. Online: http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived

[11] Summers, Nick. "New Tinder Security Flaw Exposed Users' Exact Location for Months," *BloombergBusinessweek*. February 19, 2014. Online: http://www.businessweek.com/articles/2014-02-19/new-tinder-security-flaw-exposed-users-exact-locations-for-months

[12] Federal Trade Commission. "Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False," Press Release. May 8, 2014. Online: http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

Investigations by the *Wall Street Journal*,[13] the U.S. Government Accountability Office[14] and the Federal Trade Commission[15] have all found that the collection and sharing of consumers' location data is widespread and often occurs without their consent.

Current Laws Have Failed to Keep Pace With the Rapid Evolution of Location-Based Services

The consensus among consumer privacy advocates and government officials is that there is no adequate legal framework protecting consumers' most sensitive data, including location data, in the current and ever-evolving mobile ecosystem. No federal law requires companies to obtain consumers' permission before sharing location data collected from users' mobile devices. Absent such legislation, consumers are left to rely for their protection on self-regulation by mobile phone

---

[13] Thurm, Scott and Kane, Yukari Iwatani. "Your Apps Are Watching You," *The Wall Street Journal.* December 17, 2010. Online: http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704694004576020083703574602.html

[14] *See e.g.*, U.S. Government Accountability Office. *Mobile Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, pg. 19. September 2012. Online: http://www.gao.gov/assets/650/648044.pdf

[15] Federal Trade Commission. "FTC's Second Kids' App Report Finds Little Progress in Addressing Privacy Concerns Surrounding Mobile Applications for Children," Press Release. December 10, 2012. Online: http://www.ftc.gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing

providers and app developers, as well as outdated and vague laws that may or may not apply to location data collected via mobile devices.

For example, the Electronic Communications Privacy Act (ECPA) prevents companies that collect location information from a smartphone (e.g. mobile operating system providers, application developers, and wireless carriers) from sharing that information with the government without consumer consent. However, under ECPA there is virtually no legal restriction on businesses' ability to share location data obtained from mobile devices with other, non-governmental, third parties.[16]

Similarly, the Telecommunications Act of 1996 and the Cable Communications Policy Act of 1984 prohibit telecommunications providers from disclosing customer proprietary network information (CPNI), including "location —information that relates to the . . . location . . . [of] any customer of a telecommunications carrier . . . that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[17] Except in certain narrow instances (such as in emergency contexts), the CPNI rules provide privacy

---

[16] *See, e.g.* Statement of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice before the Subcommittee on Privacy, Technology and the Law of the Committee on the Judiciary, United States Senate. May 10, 2011. ("It [ECPA] places a great deal of restrictions on the ability of providers to share that information with the Government, but virtually no legal restriction on providers' ability to share that with other third parties.") Online: http://www.gpo.gov/fdsys/pkg/CHRG-112shrg86775/html/CHRG-112shrg86775.htm

[17] 47 U.S.C. § 222.

protections for location information transmitted by a consumer's mobile device in the course of a telephone call. However, if that same device were to then be used to transmit location data via the wireless carrier's mobile broadband network (such as via a mapping app), the privacy of that data would *not* be protected the CPNI rules do not apply to location data collection independent of the telecommunications carrier's network.

Finally, the Federal Trade Commission (FTC) has been seen as the default privacy regulator for most consumer data under the FTC Act's prohibition on unfair and deceptive trade practices.[18] Indeed, the FTC has brought numerous enforcement actions against companies that have failed to live up to their privacy policies with regards to the collection and sharing of location data (e.g. Snapchat, Brightest Flashlight). However, under current law, if companies affirmatively state in their privacy policies that they will collect and share their users' location data without consent with any third party they wish, they are free to do so and the FTC has little power to stop them. As long as a company is not violating its own privacy policy, the FTC or state Attorneys General would likely have no grounds to bring a case. Given the sensitivity of location data, the limited resources of state and federal enforcement agencies and the lack of a comprehensive privacy framework, we need the affirmative rules governing the sharing of location data that S. 2171 provides.

[18] 18 U.S.C. § 1030

Industry Self-Regulation Has Failed to Adequately Protect Consumers' Location Data

Absent a clear legal framework regarding location privacy, businesses have relied on a variety of often voluntary and inconsistently applied company policies and industry best practices.

For example, Apple contractually requires that app developers using its app store obtain users' consent before collecting or disclosing location information to third parties and provide disclosure regarding the use of location-based data.[19] Google requires users to provide opt-in consent before location information can be collected by its Android operating system during the initial set-up process for a smartphone or other mobile device.[20] However, Google does not control the use of location data by third-party applications using a device running the Android operating system.[21]

---

[19] Letter from Bruce Sewell to The Honorable Edward J. Markey and the Honorable Joe Barton. Pg. 10. July 12, 2010. Online: http://www.wired.com/images_blogs/gadgetlab/2011/04/applemarkeybarton7-12-10.pdf#page=10

[20] *See, e.g.* Testimony of Alan Davidson, Director of Public Policy, Google Inc. Before the U.S. Senate Committee on Commerce, Science and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance. Pg. 5. May 19, 2011. Online: https://docs.google.com/a/nclnet.org/file/d/0BwxyRPFduTN2ZTJjYzA4YjltZTc0Ni00ZjQ3LTk1YTYtZDFiMzkwMGY1NTYx/edit?hl=en

[21] *Ibid.* Pg. 7.

Similarly, a GAO study of in-car location based services found that despite recommended practices, location data disclosures were often broadly worded and inconsistently described the purposes for sharing de-identified location data. In addition, the GAO study noted that the in-car services had inconsistent policies or failed to follow industry best practices with regards to location data retention, data deletion and accountability disclosure.[22]

Multi-stakeholder agreements, such as the National Telecommunications and Information Administration's (NTIA) short form notice code of conduct to promote transparency in mobile applications[23] and Future of Privacy Forum's Mobile Location Analytics Code of Conduct[24] may provide a forum for industry self-regulation in the area. However, the voluntary nature of multi-stakeholder agreements and industry best practices limits their value in protecting consumers in the rapidly growing mobile data ecosystem.

---

[22] United States Government Accountability Office. *In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers* (GAO-14-81). Pg. 12-20. December 2013. Online: http://www.gao.gov/assets/660/659509.pdf

[23] National Telecommunications & Information Administration. *Short Form Notice Code of Conduct To Promote Transparency in Mobile App Practices.* Redline Draft. July 15, 2013. Online: http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf

[24] Future of Privacy Forum. "Future of Privacy Forum Partners with The Wireless Registry to Create Central Location Analytics Opt-out Service," Press Release. February 18, 2014. Online: http://www.futureofprivacy.org/wp-content/uploads/FINAL-PRESS-RELEASE.pdf

The Location Privacy Protection Act of 2014 Is a Critically Important Consumer Protection Measure For Meeting the Privacy Challenges of Today's Rapidly Evolving Mobile Data Ecosystem

While NCL supports a comprehensive legal framework to protect the privacy of *all* consumer data, absent Congressional action to create such a framework, steps should be taken to protect especially sensitive types of information such as location data. Such action is appropriate and would be consistent with other areas in which Congress has recognized the sensitivity of certain types of consumer data such as health care (the Health Insurance Portability and Accountability Act's Privacy Rule[25]), financial services (the Gramm-Leach-Bliley Act's Financial Privacy Rule[26]), children's data (Children's Online Privacy Protection Act[27]) and videotape rental and sales records (Video Privacy Protection Act[28]).

As consumer surveys demonstrate, consumers are worried about the use of their location data and want greater understanding of and control over what they share with businesses in the mobile data ecosystem. It is also apparent that the combination of current law and industry best practices has failed to meet this need. Congressional action is clearly necessary to address the gaps in the law that make it impossible to provide robust consumer protections for sensitive location data.

---

[25] 45 C.F.R. Parts 160 and 164, Subparts A, C, and E

[26] 15 U.S.C. §§ 6801–6809

[27] 15 U.S.C. §§ 6501–6506

[28] 18 U.S.C. § 2710

This pro-consumer and pro-privacy bill would help to restore consumer trust in location-based services and ensure that the many benefits of this technology continue to flow to consumers and the economy. The need for this bill has been amply demonstrated via recommendations from the GAO, FTC and consumer and privacy advocates.

In particular, we believe that the bill's opt-in provisions will give consumer the information they need to make an informed decision regarding the use (or not) of location-based services on their mobile devices. Requiring up-to-date disclosures of how location data are being used, coupled with an opportunity to opt-out at a later date, gives consumers needed and ongoing control over their data.

By prohibiting so-called "stalking apps," the law will appropriately outlaw a class of inherently deceptive and predatory applications that compromise the personal safety of some of our most vulnerable citizens. No federal law currently prohibits the operation of such apps, which are designed to run secretly without the user's knowledge.

This bill would not, as some have argued, create an undue burden on innovators.[29] Indeed, if that were a real threat, NCL would not support this effort.

---

[29] Josten, R. Bruce. "Letter Opposing S.1223, the 'Location Privacy Protection Act of 2011,' and Substitute Amendment," U.S. Chamber of Commerce. December 4, 2012. Online:

Fortunately, the LPPA simply closes loopholes in existing law and levels the playing field to ensure that all mobile device applications and services play by a standard set of consumer protection rules. Responsible application service providers such as Apple and Google already require or at least strongly recommend that mobile applications respect the sensitivity of consumers' location data. This bill would simply give those best practices the force of law, creating a strong incentive for application developers and others to use location data responsibly. The bill also gives the FTC discretion to craft rules that preserve the benefits of location-based services and avoid redundant notifications to consumers.

Protections such as those embodied in S. 2171 would be of little use without effective enforcement mechanisms. We therefore support the bill's provisions establishing clear enforcement authority for the Department of Justice. S. 2171 is in line with similar consumer protection laws such as ECPA. In addition, we strongly believe that the creation of a private right of action is imperative. Given the limited resources of federal enforcement agencies, an appropriately defined private right gives an extra layer of protection to consumers. The granting of a private right of action will not, as some have argued, squelch innovation.[30] For example, the Stored

---

https://www.uschamber.com/letter/letter-opposing-s1223-%E2%80%9Clocation-privacy-protection-act-2011%E2%80%9D-and-substitute-amendment

[30] *See, e.g.* U.S. Chamber of Commerce. "Letter Opposing S. 1223, the 'Location Privacy Protection Act of 2011,' and Substitute Amendment," December 4, 2012. Online: https://www.uschamber.com/letter/letter-opposing-s1223-%E2%80%9Clocation-privacy-protection-act-2011%E2%80%9D-and-substitute-amendment

Communications Act[31] and the Video Privacy Protection Act[32] both have had uncapped private rights of action (as opposed to the $2 million cap for willful violations proposed in S. 2171). While these laws were in place the Internet economy and online video services such as YouTube and Netflix have flourished.

Conclusion

In closing, I would like to reiterate NCL's strong support for S 2171. In today's ever-changing digital economy, consumers expect and deserve that the privacy of sensitive data such as their location information will be protected. Absent such protections, consumers may indeed become less trusting in location-based services, which would be hugely harmful to innovation and the broader economy.

Mr. Chairman, Mr. Ranking Member and members of the subcommittee, on behalf of the National Consumers League and America's consumers, I applaud your leadership in convening this hearing and your invitation to testify on this important issue. I look forward to answering any questions you may have.

Thank you.

---

[31] 18 U.S.C. Chapter 121 §§ 2701-2712

[32] 18 U.S.C. § 2710

PREPARED STATEMENT OF ROBERT D. ATKINSON

Dr. Robert D. Atkinson

President and Founder

Information Technology and Innovation Foundation (ITIF)

"The Location Privacy Protection Act of 2014"

Submitted to

The U.S. Senate Committee on the Judiciary

Subcommittee on Privacy, Technology and the Law

June 4, 2014

Chairman Franken, Ranking Member Flake, and members of the Committee, I appreciate the opportunity to submit testimony regarding the Location Privacy Protection Act of 2014. I am the President of the Information Technology and Innovation Foundation (ITIF). ITIF is a nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity.

The proposed legislation addresses two very distinct and unrelated issues relating to the use of geo-location data: 1) the collection and use of personal geo-location data by third-parties, and 2) the collection and use of personal geo-location data by individuals, especially in situations that might perpetuate domestic violence, stalking, and harassment. Since these issues are unrelated I will address each separately.

Limiting the Collection and Use of Geo-Location Data by Third Parties Would Unnecessarily Stifle Innovation

The last few years have seen tremendous growth in innovation around location-based services driven by the availability of low-cost mobile devices and ubiquitous wireless connectivity. Location-based services use data about the location of a user's electronic device to deliver personalized applications and services, such as location-based social networking, entertainment, personal fitness, dating, advertising, and search, among many others. These location-based services may use a variety of techniques, including GPS and triangulation from cell towers or Wi-Fi networks, to determine an individual device's location. In addition, other techniques such as using IP addresses or user-submitted information may be used to identify a less-precise estimate of a device's location. The proposed legislation addresses the use of geo-location data that is sufficient to identify the street and city where the device is located.

First, given the rapidly developing nature of the market for location-based services it would be premature to pursue legislative changes to create a new set of rules to govern the technology. While there has been substantial change in the market for location-based services in the past few years, another wave of location-based services are likely to emerge in the coming years as a result of multiple technology trends, including the growth in adoption of in-car navigation and "infotainment" systems; connected devices making up the "Internet of Things"; and facial recognition systems. Dynamic technologies that are quickly evolving in response to changes in technological capabilities, consumer demands, and cultural norms do not lend themselves to the slower-moving regulatory process of Congress and federal agencies. A better approach is to rely on industry-led self-regulatory efforts which can more rapidly address potential consumer concerns while also being responsive to changes in technology and the private sector.[1] Government oversight and enforcement by agencies such as the Federal Trade Commission (FTC) supplements these efforts to ensure their effectiveness and accountability.

Self-regulation is already used in areas such as online advertising to govern how geo-location data may be used and shared with third parties. For example, the Digital Advertising Alliance's Self-Regulatory Principles has strong transparency requirements stating that mobile apps must give "clear, meaningful, and prominent" notice if transferring geo-location data to third-parties.[2] Other industry-led efforts have also been effective at addressing many of the most common concerns about the most common uses of geo-location data. For example, the two major mobile device operation systems—iOS and Android—allow users to see whether an app uses geo-

location data both before downloading an app and after installing it. In addition, users can disable location services completely for their devices and for each individual app on their device. These types of settings allow users who are concerned about the privacy of their location data to make informed choices about whether it is disclosed.

Codifying current practices in legislation limits the ability to introduce future innovation, including new business models and new technologies. For example, while it is fairly straightforward for mobile apps to provide notifications to users on mobile devices via their touchscreens, not all connected devices in the future will have these types of interfaces. The coming years will likely see a rapid development in connected devices that will make up the Internet of Things, including connected vehicles and wearable computing, and many of these will use geo-location data. It is not obvious how developers of a product like "smart" shoes that collect geo-location information would comply with the notification and consent requirements in the proposed legislation. (Such "devices" could be covered under the legislation since they are "commonly carried by or on the person of an individual".) While these types of devices are less common today, this may not always be the case, and legislation should not preempt these types of products at such an early stage in their development.

Moreover, while notification and consent to use geo-location data is appropriate for mobile apps today, it may not be so for other types of platforms in the future. For example, the use of geo-location information may be so integral to the purpose and functioning of a particular device that mandatory disclosures and consent requirements would be superfluous. The success of products and services often depends, in part, on how easy they are to use. Consumers expect products and services to just work immediately "out of the box." As norms change, many consumers will likely come to expect apps to deliver personalized content based on a variety of information, including their location. Unnecessary alerts, consent requirements, and disclosures make it more difficult to enroll new customers and create a "speed bump" for innovation.

Second, there is little evidence of any actual harms arising from the commercial use of geo-location data. Much of the concern expressed to date by privacy advocates stems from speculative harms, not actual ones. In fact, companies collecting and using the data have strong incentives to not harm consumers, either directly or indirectly, since doing so would badly damage both their reputations and commercial prospects. This is not to say that some companies have not made some mistakes as they seek to innovate, but there is no evidence that these mistakes are either purposeful or a result of negligence. Rather, they reflect that fact that innovation, especially in new spaces like location-based services, is complex and often difficult.

Third, the proposed legislation could discourage many innovators from bringing location-based products and services to the market. The legislation would create a private right of action and allow fines of up to $2 million for violations in how a company discloses or obtains consent about the use of geo-location information, in addition to potentially requiring the defendant to pay the plaintiff's attorney's fees. These stiff penalties, coupled with the motivation for trial lawyers to find and bring cases, will make many risk-averse companies, particularly small companies and startups, avoid using geo-location data in their mobile apps and other devices for fear that inadvertent mistakes could end up with them facing significant liabilities for fines and legal fees, which in many cases would lead to personal bankruptcy.

The consent requirements would also impair the use of geo-location data in some situations. For example, Carrier IQ is a diagnostics and analytics software tool that many carriers install on mobile devices to better understand their customers, the devices used on their networks, and the performance of their networks. Carrier IQ collects data such as when and where calls fail; where customers have problems accessing the network; and the reliability and battery performance of the make and model of devices. This information is then used to improve service quality and answer consumer questions. For example, a service provider's technical support staff can use this data to help better understand and resolve customers' issues, such as a mobile device losing connectivity in a certain location or a tablet PC's battery draining too quickly. If consumers have to opt in to this type of service there will be a strong incentive to "free ride" by not contributing their own data but still benefiting from the overall health of the wireless network based on the information collected from others. Of course, if a significant number of users do not use this type of service all users will suffer the consequences. The same is true with regard to traffic flow data where de-identified data is used to enable real-time traffic maps on roadways; if some individuals opt out, the overall quality of the data for all travelers will decline.

Another type of use that might suffer under this legislation is the use of geo-location in online advertising. Online advertising pays for a significant amount of free content and services that consumers enjoy, including mobile apps. In 2013, online advertisers spent approximately $43 billion, including $7 billion on mobile advertising.[3] However, advertisements need to be effective to justify these significant outlays. This means that advertisers need to be able to use data to deliver relevant advertising and use data to analyze the effectiveness of advertising. Apps that require users to grant them a greater number of permissions are less likely to be downloaded. Requiring apps to get give notices to users about use of geo-location data in advertising would force many developers to make the tradeoff between incorporating useful location data, either to be used directly by the application or for third-party advertising, and potentially scaring off customers. Moreover, many apps are using geo-location data to deliver more relevant advertising to consumers. For example, apps like Yelp and FourSquare allow restaurants and retailers to offer promotions to customers who "check in" to a specific location, and the car service Uber runs promotions to its users based on their geo-location, such as a special discount for attendees at certain events. Geo-location data may also be used to be more sensitive to when customers are shown advertising, such as avoiding showing ads when someone is visiting a cemetery. The effect of limiting the relevance of ads, besides consumer inconvenience, would be to reduce revenues going to the mobile ecosystem, with the result being either fewer or lower quality apps or fewer free apps.

In addition, some of the components of the bill are particularly problematic. The requirement that companies disclose the name of every third party they share geo-location data with, as opposed to general categories of reasons for data sharing, would mean that companies would risk sharing proprietary information about their business models to their competitors.

Limiting the Collection and Use of Geo-Location Data by Individuals Would Be Insufficient to Fully Address Concerns about Domestic Violence, Stalking, and Harassment

Domestic violence, stalking, and harassment are serious issues, and ITIF applauds the Committee's efforts to address this ongoing concern. Unfortunately, the provisions in the proposed legislation, while helping with the problem, will likely not be sufficient to fully address

it, may interfere with legitimate tracking applications, and could require changes in mobile operating systems.

First, the legislation includes a number of "anti-stalking provisions" that might be useful for apps that collect and report back to users their geo-location information, but would be applied too broadly to all apps using geo-location data. For example, the legislation requires that users be alerted after more than 24 hours but before 7 days that their geo-location information is being collected. As written, this provision would apply to many different background apps that use location-based services, not just "stalking apps." For example, Passbook is an app on iOS that organizes information, such as boarding passes, movie tickets, and gift cards, and then presents that information automatically to the user when they arrive at the associated location (such as an airport).[4] This type of app runs in the background and is arguably "imperceptible to the user", thereby meeting the definition of the proposed legislation. Delayed notification that geo-location information is being collected for this type of app does not make sense and will only serve to confuse users. Indeed, most apps that collect geo-location information, such as weather or traffic apps, do not allow the individual user to gain access to the information. This is in contrast to apps like Amber Alert GPS Teen, that lets parents download a tracking app on their children's mobile device and track the device's location. As such, we recommend that if the Committee moves forward with this provision, it only apply the 24 hour-7 day second notification rule to apps where individuals can gain direct access to the location data.

Second, even requiring apps to display a delayed notice, however, may not limit stalkers. This is because the delayed notification requirement presents a technical challenge since both the Android and iOS operating systems allow users to turn off notifications.[5] In other words, a stalker who places a tracking app on another person's mobile device could simply shut off notification from that app. For the after-installation notice provision to be fully effective, this legislation would need to require changes to these operating systems to allow third-party app developers to override user preferences about notification settings. Moreover allowing developers to override user preferences could result in a degraded mobile experience as developers may provide notices to users who do not want them and decide to start showing users other notifications, not just geo-location privacy notices.

Third, because the Internet is global, even if Congress successfully bans tracking apps in the United States, users will still likely be able to access them on foreign web sites. This is particularly problematic for mobile devices that allow apps to be installed from any location (i.e. not just from an "authorized" app store). For example, a foreign app store may sell apps that are designed to help parents keep track of their teenage children but that does not include the 24 hour-7 day second notice requirement In some cases it may be appropriate for the U.S. government to require that access to certain websites be blocked (such as a website only selling apps that are illegal in the United States), but in other cases, such as when a site is selling many different apps and products and the vast majority are lawful, it would be inappropriate to block access on such a wide scale.

Fourth, even if the delayed notification provision does help with regard to mobile apps, there are other technologies that stalkers can use, such as portable GPS devices, many of which are used for legitimate purposes. For example, the Amber Alert GPS Smart Locator is a standalone device that parents can place in a child's backpack in order to keep track of the child's location.

These same devices could also be placed in a person's car by a stalker. It is not clear how these devices could meet the notification and consent requirements in the legislation.

Fifth, as this above example illustrates, at a technical level there is little difference between a stalking app and a legitimate app that tracks an individual device's location and reports this information to that individual or another user. Legitimate examples of tracking include apps designed to find lost or stolen electronics, apps designed to create a "geo-fence" for teenage drivers, and apps designed to track the location and safety of loved ones who are unable to live independently, such as parents with early stages of dementia or adults with cognitive disabilities. In particular, some parents have troubled children who they may feel they need to track to provide proper supervision. If the children know that they are being tracked, they may simply leave their phone at home, school or with a friend. This is not to say that this provision should not be enacted, only that it would also prevent this kind of beneficial tracking without the person's knowledge.

Unfortunately, it is virtually impossible to restrict one type of tracking app but not another. Congress could and should ban the marketing and sale in the United States of apps advertised and marketed as stalking apps, but that would not prevent would-be stalkers from using a legitimate tracking app for "off-label" purposes. Moreover, tracking itself is not a problem; rather, the problem is its use by stalkers. After all, a number of apps use geo-location data to protect the personal safety of individuals, such as by sharing personal geo-location data with trusted friends and family. One mobile app, which was a winner in the 2011 HHS / White House "Apps Against Abuse" Challenge, allows users to quickly and surreptitiously request that friends pick them up by sharing their precise geo-location.[6] Another app, the "Safety Siren", developed by YWCA Canada, allows users to quickly send a text or email to friends with their location information if they are in an unsafe situation.[7] Some states have begun to use geo-location data to turn the tables on stalkers and ensure that victims and police are alerted of possible threats. As of 2012, at least twelve states already have laws that require certain offenders to wear a tracking device so that police and victims can be alerted if the offender violates a protective order.[8] ITIF encourages Congress to consider efforts to expand the number of states using GPS tracking devices to protect those individuals threatened with domestic violence or other illegal harassment, including through grants from the Department of Justice.

In addition, Congress should be aware that advances in mobile security may help address some of the concerns about surreptitious stalking apps. These types of apps are a form of malware—malicious programs installed without the users knowledge. There are other types of malware including keyloggers (that steal private information, such as credit card numbers and passwords) as well as backdoors that allow remote access to a device. Many users are concerned about these types of security threats and developers are responding by developing improved security tools for mobile devices. In the coming years, we will likely see more anti-virus and anti-malware tools for mobile devices just like there are for PCs. These tools will likely address a variety of malware threats, including stalking apps. In addition, mobile operating system developers will continue to add new security features, such as biometric authentication requirements that would help prohibit apps from being installed on a user's device without their biometric "permission."

In the short term, individuals concerned that third-parties may have access to their mobile devices and are using this access to track them can take a number of steps to protect themselves

including changing the passwords for their mobile devices and associated accounts; installing anti-malware and anti-virus apps; and even disabling all location-based services in the mobile device's operating system. The Department of Justice should work with victims' assistance organizations to ensure that these kinds of self-help practices are widely understood.

Conclusion

In summary, geo-location data offers many opportunities for innovation in the coming years and efforts to regulate its use for commercial purposes will do little to protect consumers and are likely to limit continued innovation. In addition, the Committee should also be aware that even the stalking provisions will not be a "magic bullet" for stopping electronic stalking, in part because stalkers can turn off notification and also use other kinds of devices not covered here. Given the concerns expressed above about the impact that this legislation would have on voluntary and legitimate uses of geo-location data by third parties for innovative applications and services, I recommend the committee not move forward with Section 3 of the legislation and instead focus its efforts on criminal penalties for stalking as outlined in Section 4 and the other measures in Sections 5 through 10.

Endnotes

---

1. Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising," (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

2. "Application of Self-Regulatory Principles to the Mobile Environment," Digital Advertising Alliance, July 2013, http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

3. "2013 Internet Ad Revenues Soar To $42.8 Billion, Hitting Landmark High & Surpassing Broadcast Television For The First Time—Marks a 17% Rise Over Record-Setting Revenues in 2012", Internet Advertising Bureau, April 10, 2014, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041014.

4. For more on Passbook, see http://support.apple.com/kb/HT5483.

5. For Android see, "How To Shut Off Android Notifications," Digital Trends, September 3, 2012, http://www.digitaltrends.com/mobile/how-to-deal-with-android-notification-spam/. For iOS see, "" "iOS: Understanding notifications," Apple, January 17, 2014, http://support.apple.com/kb/ht3576.

6. See Circle of 6 at http://www.circleof6app.com/.

7. See YWCA Safety Siren at http://ywcacanada.ca/en/pages/mall/apps.

8. Daniel Castro, "Location Privacy Legislation is Move in Wrong Direction: Part 2 – Stalking and Domestic Violence", Information Technology and Innovation Foundation, January 14, 2013, http://www.innovationfiles.org/location-privacy-legislation-is-move-in-wrong-direction-part-2-stalking-and-domestic-violence/.

PREPARED STATEMENT OF CINDY SOUTHWORTH

NNEDV
NATIONAL NETWORK TO END DOMESTIC VIOLENCE
1400 16TH STREET NW SUITE 330 WASHINGTON, DC 20036
www.nnedv.org phone: 202.543.5566 fax: 202.543.5626

The Testimony of
the National Network to End Domestic Violence
with the Minnesota Coalition for Battered Women

Cindy Southworth, MSW
Vice President of Development and Innovation
and Founder of the Safety Net Technology Project at NNEDV

June 4, 2014
Hearing of the Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
United States Senate
Location Privacy Protection Act of 2014

A few days before this hearing[1], I received a phone call from Harriet, a 74-year-old retired teacher in California, who heard from her advocate that I was collecting stories about how victims are being impacted by location tracking. This is Harriet's story: Harriet met a charming man in a grief support group and they began dating. He gave her a cell phone. She protested that it was too expensive, but he insisted she accept his gift and use the phone. Things escalated and then he raped her, after which she refused to see him again. He felt no remorse after the assault and called her incessantly and showed up wherever she went. It was uncanny that he knew everywhere she would go – causing her to feel hunted. She turned off the "gifted" phone to experience some relief from his control, but every time she turned it on to see if her family had called, her offender would call moments after she powered on the phone. When she reached out for help, she received a temporary protection order, but unfortunately the judge denied the permanent order saying "there wasn't enough evidence." Her only recourse was to leave her community, her friends, and her support system. She called me in hopes that her story could help others. The strength and resilience of Harriet and all survivors inspires me every day.

I. Introduction

Good afternoon Chairman Franken, Ranking Member Flake, and distinguished Members of the Committee. Thank you for inviting me to testify about the importance of location privacy and transparency for victims of domestic violence, sexual assault, and stalking. My name is Cindy Southworth and I am the Vice President of Development and Innovation at the National Network to End Domestic Violence.[2] I am also representing our member, the Minnesota Coalition for Battered Women.[3] I am testifying today on behalf of Harriet and the 7 million victims each year who are assaulted, raped, or stalked by a current or former partner.[4]

[1] Conversation with "Harriet" (name changed to protect the victim's confidentiality) on May 31, 2014.

[2] NNEDV is a social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1990 and officially incorporated in 1995, NNEDV represents 56 state and territory domestic violence coalitions who in turn represent nearly 2,000 local domestic violence service providers across the country.

[3] The Minnesota Coalition for Battered Women is a well-established, membership organization with over 80 local, regional, and national member programs located throughout Minnesota. The Coalition has existed for 35 years as the state's primary voice for battered women and has a strong history of effectively carrying out public policy that advances women's safety and security.

[4] U.S. Department of Justice, National Institute of Justice and Centers for Disease Control and Prevention. (July 2000). Extent, Nature, and Consequences of Intimate Partner Violence: Findings From the National Violence Against Women Survey. Washington, DC. Tjaden, P., & Thoennes, N.

[5] Cindy Southworth, the Vice President of Development and Innovation at the U.S. National Network to End Domestic Violence (NNEDV) leads the technology, communications, development, and finance efforts of NNEDV. She joined NNEDV in 2002 when she founded the Safety Net Technology Project to address the intersection of technology and violence against women. Through the Safety Net Project, Ms. Southworth works with private industry, advocacy organizations, law enforcement, state and federal agencies, and international groups to improve safety and privacy for victims in this digital age. She has presented over 460 trainings to more than 35,400 advocates, technologists, and justice professionals, including over 25 international presentations and keynote addresses. She has testified before Congress and is on many task forces and committees that address justice, privacy, technology, and safety. Ms. Southworth has a Master's Degree in Social Work and has worked to end violence against women for over 20 years at national, state, and local advocacy organizations. She has spent the past 16 years focusing on how technology can increase victim safety and how to hold perpetrators accountable for misusing technology. Ms. Southworth also serves on the Airbnb's Trust Advisory Board and the Advisory Boards of MTV's A THIN LINE digital abuse campaign, the Privacy Rights Clearinghouse, and the Computers Freedom and Privacy Conference. The NNEDV Safety Net Project is one of 5 organizations internationally that serves on the Facebook Safety Advisory board.

Summary of Issues

1) Domestic Violence and stalking impact the entire community at epidemic rates. 1 in 3 women will be assaulted by an intimate partner in her lifetime. 1 in 6 women will be a victim of stalking in her lifetime.
2) Location information about victims of domestic violence and stalking is undeniably sensitive, thus surreptitious location tracking devices and apps disproportionately dangerous for these individuals.
3) If a victim knows she/he is being tracked or monitored, she/he can take steps to mitigate risk (e.g., leave compromised phone or tracked car at home when she files a police report or meets with a victim advocate).
4) National data collected in 2006 (1 year before the iPhone was released, 2 years before the App stores were opened) indicates that Global Positioning Systems (GPS) tracking and electronic monitoring impacted thousands of victims that year, long before the proliferation of "apps." Eight years later, ninety percent of American adults have a cell phone—the majority of which (58%) are smartphones. A 2012 NNEDV survey of victim service providers around the country found that 72% of them had seen victims who were stalked through the use of a stalking app or GPS or location tracking device.
5) If location tracking technology is being used legitimately to monitor children or employees, there is no need for a "stealth mode" or for it to run invisibly. Many reputable family safety and location sharing social networks only function with full notice, consent, and visibility.
6) Location tracking technology designed to run in stealth mode is being designed to facilitate stalking and spying. Often these products are marketed to "spy on" or "stalk" your girlfriend/partner/spouse.
7) Many vendors boast about the ability to track your girlfriend, partner, or spouse without the victim's knowledge. Some vendors claim their location tracking product is for monitoring employers or children, yet have the same stalking-focused features as the blatantly advertised "stalking apps."

Summary of Solutions:

A. Impose criminal penalties on individuals who use mobile technologies to spy on or stalk individuals.
B. Require a reminder when location is being used in the background. Abusers and stalkers often consent to the installation of stalking apps on a victim's phone, and a reminder of the tracking is needed at a future point in order for a stalking victim to become aware of this surreptitious and dangerous location tracking.
C. Criminalize the operation, sale, and marketing of technologies whose primary purpose is to surreptitiously track someone's location and facilitate a crime
D. Allow law enforcement to seize the proceeds of those sales to fund anti-stalking efforts.
E. Require the federal government to gather more information about GPS/location stalking, facilitate reporting of GPS stalking, and prioritizing training grants for law enforcement.
F. Require the federal government to prioritize funding for GPS/location stalking prevention, awareness, and detection efforts.

I. Introduction Continued

The Safety Net Technology Project at NNEDV

Founded in 2002, NNEDV's Safety Net Project focuses on the intersection of technology, stalking, and abuse. The project works to address how technology impacts safety, privacy, accessibility, and civil rights of victims. Safety Net works with communities, agencies, and technology companies to:

- Address how technology impacts survivors of abuse and stalking;
- Educate victim advocates and other professionals on ways to use technology strategically to increase safety;

- Train criminal justice professionals on tactics of technology misuse in the context of domestic violence, sexual assault, dating abuse, and stalking;
- Advise technologists on technology risks and benefits to victims; and
- Advocate for strong policies that ensure the safety and privacy of victims.

Since 2002 the Safety Net team has presented more than 900 trainings to more than 65,000 advocates, law enforcement officials, technologists, and others regarding technology tools, online privacy, and victim safety. Of these trainings, more than 45 were presented outside the United States, including Austria, Australia, Canada, England, Ireland, Lithuania, Mexico, and Portugal. Through in-depth consultations, the Safety Net Project helps police officers and victim advocates on a range of issues, including complex technology stalking cases, implementing new technologies such as smartphone applications, and developing secure online chat systems. The Safety Net Project has responded to more than 13,500 unique requests for assistance, consultation, and resources - averaging over 100 requests each month. The Safety Net Team also works closely with technology companies such as Verizon, Google, and Facebook, and serves on Facebook's Safety Advisory Board.

Minnesota Coalition for Battered Women

The Minnesota Coalition for Battered Women (MCBW) has long been a leader in the domestic violence movement, especially with implementing legislative policy that supports and protects battered women and children. They were one of the first states to adopt a stalking statute in the early 1990s, and in 2010, the Coalition initiated and monitored the passage of several amendments to the stalking statute to update and increase protections for victims. A significant provision in this statute now includes the use of modern technologies being used as a means to stalk a victim. The Minnesota stalking statute (MN Stat §609/748 sudb. 2(6)) specifically states that it is a criminal act of stalking if a person *"repeatedly mails or delivers or causes the delivery by any means, including electronically, of letters, telegrams, messages, packages, through assistive devices for the visually or hearing impaired, or any communication made through any available technologies or other objects."* The Coalition supported the passage of this provision because they received reports from battered women throughout the state that modern technology was being misused by abusers to stalk victims.

Everyone Knows a Survivor: Prevalence and Impact

- 1 in 3 women will experience an assault by an intimate partner at some point in her lifetime.[6]
- 1 in 6 women and 1 in 19 men who will experience stalking in her and his lifetime.[7]
- Seventy-eight percent of stalking victims are women.[8]
- More than half of victims reported losing 5 or more days of work due to stalking, and 130,000 victims reported that they had been fired or asked to leave their job due to stalking.[9]
- A study found that one-fourth of stalking victims reported financial control by the stalker. Sixty-eight percent of the stalkers controlled the victims socially. Virtually all stalkers (98%) attempted to control the victim psychologically.[10]

---

[6] Black, M.C., Basile, K.C., Breiding, M.J., Smith, S.G., Walters, M.L., Merrick, M.T., Chen, J., & Stevens, M.R. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

[7] Katrina Baum et al., "Stalking Victimization in the United States," (Washington, DC: Bureau of Justice Statistics, 2009).

8 Seventy-eight percent of stalking victims are women. Center for Policy Research (1997). Stalking in America.

9 Baum, K., Catalano, S., Rand, M., and Rose, K. (2009) Stalking Victimization in the United States. Bureau of Justice Statistics.

10 Brewster, M. (2003). Power and Control Dynamics in Prestalking and Stalking Situations. Journal of Family Violence. 18(4).

In Just One Day
In just one day in the United States, more than 64,000 adults and child victims are helped by almost 2,000 local domestic violence shelters and outreach offices. Tragically, almost 10,000 times in the same day, a victim found the courage to tell a complete stranger about the abuse perpetrated by someone who was supposed to love her and the overworked and underpaid advocate was forced to say "I am SO sorry, but we don't have a bed/attorney/counselor available."[11]

Homicide Risk
Abusers and stalkers go to great lengths to maintain power and control over their victims. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the abuser.[12] Many victims are stalked relentlessly for years after having escaped from their partners. Batterers who stalk their former partners are the most dangerous and pose the highest lethality risk.[13] In fact, 54% of femicide victims reported stalking behavior to the police before the victims were killed by their stalkers.[14] Nationwide, an average of 3 women are killed by a current or former intimate partner every day.[4]

Technology Stalking Statistics
It is nearly impossible for the average American to go about his or her daily life without using technology. Technology has become much more than just a convenience or a form of entertainment. Technology is a tool to connect with friends and family, to complete daily tasks, and to educate and learn, whether it's "to Google" or to take online classes. Americans are increasingly connected – 87% of adults use the internet[15] and are progressively doing more using mobile devices. Ninety percent of American adults have a cell phone (the majority of which (58%) are smartphones) that are being used to go online (63%), download mobile applications (50%), and much more.[16] Domestic violence and stalking occur where we live our lives. For approximately 90% of Americans, that means in person, on mobile phones, and online since the digital world and non-digital world are now so interconnected.

The Department of Justice Office on Violence Against Women funded a Supplemental Victimization Survey to provide in-depth information about stalking. The data was collected in 2006, one year before the iPhone was released in 2007 and before the Apple and Google App stores opened in 2008. Unfortunately, this supplement has not been repeated since 2006, though smaller studies since have also indicate that technology misuse by stalkers and abusers is on the rise.

According to the 2006 data, 34% of stalking victims or a projected 1.14 million people experienced "**following** or spying," and 32% or a projected 1.04 million people experienced stalkers "**showing** up at places."[17] In the same study, 7.8% of stalking victims or a projected 246,351 people reported in 2006 that they had been victims of "Electronic Monitoring" and more than 26,000 were projected to have been

---

11 National Network to End Domestic Violence, Domestic Violence Counts: a National Census of Domestic Violence Shelters and Services. March 5, 2014. www.nnedv.org/census

12 Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).

13 Jacqueline Campbell, "Prediction of Homicide of and by Battered Women", *Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995). Also: Barbara J. Hart, "Assessing Whether Batterers Will Kill,"(1990) Available at: http://www.mincava. umn.edu/ hart/lethali.htm),

14 Judith McFarlane et al., "Stalking and Intimate Partner Femicide," *Homicide Studies* 3, no. 4 (1999).

15 Pew Research, Internet Project, "Internet User Demographics," www.pewinternet.org/data-trend/internet-use/latest-stats/

16 Pew Research, Internet Project, "Mobile Technology Fact Sheet," www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

17 Catalano, Shannan U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics "Stalking Victims in the United States – Revised" September 2012.

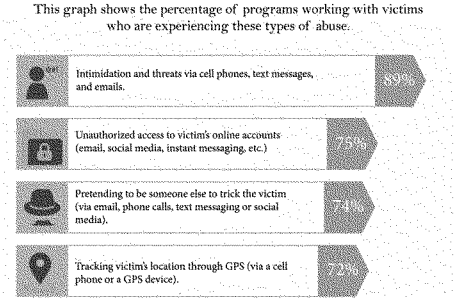
stalked specifically by GPS.[18] Since 2006, the spying and stalking apps have flooded the marketplace, making it even easier for abusers to purchase, install, and stalk. With the growing use of location technology, perpetrators are tracking victims' location more often and in increasingly varied ways.

In 2010 the Centers for Disease Control issued its National Intimate Partner and Sexual Violence Survey. It found that 38.6% of female domestic violence victims and 31% of male victims were "watched, followed or tracked with a listening or other device." (Note that this survey conflated wiretapping and eavesdropping apps with GPS/location stalking apps).[19]

In a 2012 survey of over 750 agencies conducted by NNEDV,[20] the vast majority of victim service providers reported that survivors experienced some kind of technology misuse and are asking for help dealing with technology-related abuse:

%of Programs Reported:	Survivors Report the Following Abuse
89%	Abusers harass victims via cell phone
75%	Abusers access victims online accounts without permission
72%	**Abusers track victims via GPS**

% of Programs Reported:	Survivors Ask for Help on the Following Issues
71%	Safety strategies on using their cell phones safely
62%	Help on managing location privacy
54%	Help on using online spaces/social media safely and privately



[18] Ibid.

[19] Black, M.C., Basile, K.C., Breiding, M.J., Smith, S.G., Walters, M.L., Merrick, M.T., Chen, J., & Stevens, M.R. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

[20] NNEDV, "New Survey: Technology Abuse & Experiences of Survivors and Victim Service Agencies," www.ovc.gov/news/grantees.html and http://techsafety.org/blog/2014/4/29/new-survey-technology-abuse-experiences-of-survivors-and-victim-services (data collected in 2012)

Benefits of Location Technology

Although abusers misuse technology with the intent to stalk and control, the benefits of GPS are undeniable. Location technologies assist all members of the community, including victims and survivors. For example, location devices and apps provide users with maps and directions and can send alerts when hikers are lost while climbing mountains on O'ahu,[21] or help rescue people after a boating accident off the coast of Charleston, South Carolina.[22]

The use of GPS can also help victims. In March 2011, a man was arrested for kidnapping his 4-year-old son outside of a domestic violence center. Police were able to track his movements based upon his cell phone signal. He was taken into custody and the boy was returned to his mother. The man was jailed, charged for assault, and his estranged wife was granted a restraining order against him.[23]

II. The Problem: Stalking Apps and GPS Location Tracking by Abuser and Stalkers

> Last week a survivor in Indiana reached out for help from a local victim advocate. "Mary" discovered her estranged abusive husband had installed a location tracking app on her phone. She became suspicious when he always called if she varied her routine such as stepping out of her building to buy a sandwich for lunch instead of eating in the building's deli. She asked the advocate to help her figure out what app is on the phone and hoped she wouldn't have to replace her expensive smart phone.

Stalkers misuse location technology to hunt down and/or continuously monitor their victims in several primary ways, including: 1) family locator services, 2) location functionality built into the operating systems of phones, tablets, or cars 3) freestanding GPS hardware devices, and 4) stalking apps sold in App stores or downloaded elsewhere on the Internet.

1) Family Locator Services

Many products are available for the purpose of locating family members via their cell phones. Some of these products are offered through wireless carriers (e.g., Verizon Family Locator[24]). Generally, locator services provided directly from a cell phone carrier as part of a family plan require some level of authorization to access the victim's account and activate the service. Unfortunately, since most stalkers are former intimate partners, it is sometimes possible for them to find a way to impersonate the victim, access the account, and add these optional location services. Most cell phone carriers, however, have added additional authentication and verification steps, such as automatically sending a text message to the phone informing the user that a tracking application or service is enabled[25]. Without periodic notification to the tracked phone, the abuser or stalker can turn on the service and surreptitiously track and stalk another adult (the abuse victim) through the locating plan.

---

[21] A father and son hiking team were rescued from cell phone GPS after getting lost in the Koolau mountains in O'ahu, Hawaii. www.rmtracking.com/blog/2011/12/12/gps-saves-lives-in-hawaii-and-beyond/

[22] Boater Summons Rescue from US Coast Guard with SPOT Messenger April 21, 2010. www.findmespot.com/en/spotemergency/index.php?article_id=626

[23] Terry, Lynne. "Washington Police Used Cell Phone Pings to Zero in on Fugitive in Amber Alert." Oregon Local News, Breaking News, Sports & Weather - OregonLive.com. 2 Mar. 2011. Web. 26 Apr. 2011. http://www.oregonlive.com/pacific-northwest-news/index.ssf/2011/03/washington_police_used_cell_phone_pings_to_zero_in_on_fugitive_in_amber_alert.html

[24] http://www.verizonwireless.com/support/faqs/FeaturesandOptionalServices/family_locator.html

[25] https://community.verizonwireless.com/thread/201324

2) Location functionality built into the operating systems of phones and tablets or installed through a car manufacturer

Most cell phones can be tracked simply due to the way the device is designed and operated. Even without actively using the GPS in the phone, just by triangulating the cell towers—measuring the distance between the phone and the three nearest cell phone towers—the approximate location can be revealed. Wireless carrier companies also have other methods of determining a phone's location, including GPS information or network usage information that includes location (when connecting to Wi-Fi, for example). In general, the phone must be turned on and be connected with cell towers in order for the carrier to gather location information. This information is typically only available to the wireless carrier and may be obtained by law enforcement with the proper warrants or authorization.[26]

In addition to the carrier retaining location information, many phones and tablets store location history in the device itself. If an abuser or stalker is able to access the location information on the device, the offender can learn a victim's daily activities (e.g., if she met with the police or went to the courthouse to file a protection order). For example, for iPhones, the entire location history is stored under "Frequent Locations." Although there is an option to opt out of the device collecting location history, a survivor will need to know to go beyond the Location Services settings and turn off Frequent Locations under System Services. Many survivors will not know that.

Some devices also have a "find my phone" feature or are running a security software that allows the user to find their phone if it is lost or stolen. For the iPhone specifically, if the "find my phone feature" is turned on and if the abusive party has access to the victim's iCloud or online account, then they can monitor where the phone is in real time (not just historical location data), in addition to whatever information is stored in the iCloud. When NNEDV works with victims and advocates, we recommend that users put a passcode lock on their phone, and turn off location tracking in the settings if they don't need it or want it. However, with all safety strategies, survivors should only use them if it won't create suspicion from an abuser and potentially increase danger and risk.

In addition to smart phones, location information on navigational systems, such as OnStar, can be misused in order to stalk or monitor someone.[27] Family Link is an optional add-on service to the operator-assisted emergency response and navigation services offered by OnStar.[28] Subscribers can log on to OnStar's Family Link Web site to view a map with the vehicle's location at any time. They can also schedule e-mail or text alerts to update them periodically on the location of the automobile on specific days or times.[29]

> While fleeing to a Texas shelter, a victim stopped at a truck stop. OnStar disabled her car for no known reason. Police arrived and called OnStar to verify that the car was NOT stolen. The victim entered the shelter on Friday and in the middle of the night her car horn started randomly going off. It happened again each night. Monday morning, the abuser called the victim, said he knew she was staying in the shelter and threatened her. She felt protected on the secure shelter campus where her car was inside the gates, however she had to work with a local dealership and the police to get the OnStar disabled so the car horn stopped waking all of the families in shelter at 2am. ~ Advocate in Texas

[26] Lee, Kaofeng & Olsen, Erica. (2013) Cell Phone Location Privacy and Intimate Partner Violence. Domestic Violence Report, August/September 2013, Vol. 18, No. 6.

[27] Fraser, C., Olsen, E., Lee, K., Southworth, C. and Tucker, S. (2010), The New Age of Stalking: Technological Implications for Stalking. Juvenile and Family Court Journal, 61: 39–55. doi: 10.1111/j.1755-6988.2010.01051.x

[28] https://www.onstar.com/web/portal/family-link?g=1

[29] http://www.cnet.com/news/want-to-know-where-your-teen-is-ask-onstar/

3) Freestanding GPS Devices

Abusers can also use free-standing devices to monitor and stalk their victims. These GPS devices can be Portable Navigation devices (e.g., Garmin) or small tracking devices marketed to track equipment, merchandise, or equipment and be installed surreptitiously by the abusive party.

Other GPS-type tracking systems include small devices designed to be hidden under the car or inside the dashboard, and are often marketed as "Covert GPS Trackers." Some of these products are marketed for apparently legitimate use: parents can track their teens' cars to ensure that their teen goes where they say they are going and parents will be alerted if the car goes beyond a predetermined area or is speeding. Parents can reprimand their teen driver by using the product to remotely flash the dome light or honk the horn of the tracked automobile. Other products are more blatant about its purpose: Bluewater Security Professionals brazenly pitches, "By installing a vehicle tracker in the car of your husband or wife, you will be able to track their every move and tell what his or her true location is. It would be as if you were sitting right next to them in the passenger seat."

> A survivor in Missouri, "Gia" suffered years of horrific sexual violence and abuse. She was finally able to break away, moved to an undisclosed location, varies her routes to and from places, and minimized her online presence. Recently she was visiting a friend and the perpetrator showed up unexpected with a van borrowed specifically with the intention of abducting her. Fortunately she was able to escape. She has had her vehicle checked repeatedly for the tracking device that led the perpetrator to her. So far, nothing has been found on the car, so she is trying to find a tech unit that will examine her phone for her. Gia finally felt safe after years of terror and she is back to looking over her shoulder at all times. ~ Advocate in Missouri

4) Stalking apps sold in app stores or downloaded elsewhere on the Internet

One of the most comprehensive ways a stalker can track a victim is by installing a tracking program or spyware onto the victim's cell phone. In most cases the abuser will need physical access to the phone in order to install a monitoring program. This can occur if the abuser or an accomplice of the abuser has access to the phone or if the survivor inadvertently installs such a program without knowing what it does.

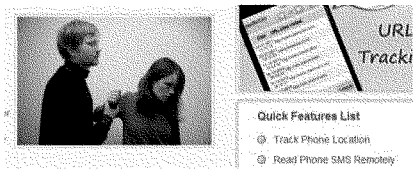
Many location tracking applications and services (some are available in app stores or via the Internet) do not provide notice to the target/victim or verify that consent to track has been obtained by the person being tracked. Stalkers can install a location-tracking application on to the victim's phone without the victim's knowledge. Depending on the type of application, the stalker can then monitor the location of the victim's phone via a website or his cell phone to monitor the real-time or historical movement of the victim's phone.

Despite the marketing claim that these location services or applications are for parents to locate their teenage children or an elderly parent, most of these services focus on the ability to operate in "stealth mode," mention that it's possible to use these services to "catch a cheating spouse," and highlight the fact that the target will not know the app is running. Most of these apps have additional features beyond disclosing the location of the cell phone. Some features allow the monitoring person (potentially, the abuser) to be notified if the targeted person goes outside of a certain geographic boundary (known as "geofencing"), be notified if the targeted person goes to or leaves a certain place or address, be sent notifications of a targeted person's location at specific times, or see a history of where the targeted person has gone throughout the day or week.

Below are two screen images of "HelloSpy," a tracking product that promises to: **"Silently monitor text messages, GPS locations, call details, photos and social media activity. View the screen and location LIVE!"** HelloSpy also claims to have over 250,000 customers, with plans ranging from $19.99/month to $119.99/year. If their numbers are accurate, this stalking app has brought in a minimum of $4,997,500 (if all customers purchased the cheapest 1-month plan).

This notable alleged "family safety" product also has a continuous animated image on their main webpage showing a scene from the movie *Cruel Intentions* where a man roughly shoves a woman off the bed, head first.[30]

On another HelloSpy webpage, there is a photo of a man grabbing a woman's forearm (see image below). The woman has visible abrasions on her face. Next to this photo is a list of the features of HelloSpy, including: Track Phone Location, Read Phone SMS Remotely, See Call History, and more.

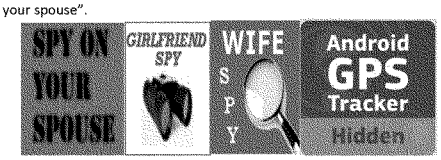


There are other apps that offer additional monitoring and spying features, in addition to location tracking. These programs are known as cell phone spyware or monitoring software. Cellphone spyware allows the abusive person to monitor all activities that occur on the phone, including all messages sent and received, apps downloaded, phone calls, voicemail received, and location information. Some spyware will even allow the monitoring person to call the phone and, without the user realizing, use the cell phone as a listening device to hear conversations occurring around the user. These products do no send any notifications to the user to inform them that their location is being tracked or even that the product is installed on their phone.

[30] http://hellospy.com/mobile-phone-spy.aspx?lang=en-US

Cellphone spyware is widely available and easy to install. The abusive person just needs a few minutes with the phone.

These apps are often brazenly marketed to stalkers, sometimes briefly mentioning employee monitoring and child safety -- almost as an afterthought or cover story -- and heavily focusing on the features that will help you "spy on your spouse".



Impact of Location Tracking by Abusers and Stalkers

As more users adopt mobile technology, abusers and stalkers are misusing that technology. The Apps and devices noted above are developed and advertised directly to stalker and certainly makes it easier to facilitate these crimes. In some tragic cases, GPS devices and apps may have actually aided the offender in locating the victim to commit murder, or the location tracking was one piece of an overwhelming list of controlling tactics that preceded a victim's death.

In 2004, a stalker in California purchased a cell phone with location tracking service expressly for the purpose of tracking his ex-partner. He attached the cell phone to the underside of her car and was only caught when the victim saw him under her car changing the cell phone's battery.[31] Numerous cases of GPS and location stalking have arisen since then.

In 2009, in Seattle, a man used the location service on his estranged wife's phone to track her to a local store. After finding her speaking to a man there, he shot and killed their five children and himself. [32]

In 2010 in Delaware a divorced father installed a GPS device on his ex-wife's car after the judge issued a Protection From Abuse Order against him. He also left 120 voicemails on his 5-year-old's cell phone in just one evening, including one where he called his daughter an "inconsiderate little bitch."[33]

In Philadelphia, on Sunday, June 20, 2010, Sean Burton installed a tracking device on his estranged wife's new partner, James Stropas' car. Between time of installation and Monday morning, the location of the device was checked via the laptop in Burton's van 147 times. Using the GPS to hunt down Stropas, Burton murdered James Stropas in a parking lot by stabbing him over 70 times.[34]

In another tragic 2010 case in Scottsdale, Arizona, Andre Leteve used the GPS on his estranged wife's phone to stalk her before he shot and killed both of their children, 15-month-old Asher and 5-year-old Alec.[35]

---

[31] Boghossian, N. (2004, September 4). High-tech tale of stalking in the 21st century. LA Daily News, p.N1

[32] Ibid.

[33] Family Court of Delaware/WestLaw/Jan. 12, 2010

[34] DiGiacomo, Marlene. Man convicted of killing Oaks resident and war vet Stropas. Montgomery News. Monday, March 28, 2011 http://www.macombdaily.com/20110325/accused-pennsylvania-murderer-recalls-bloody-struggle-with-wifes-lover

[35] Scheck, Justin. "Stalkers Exploit Cellphone GPS." Business News, Finance News, World, Political & Sports News from The Wall Street Journal - Wsj.com. 3 Aug. 2010. Web. 26 Apr. 2011.

In 2011, Dmitry Smirnov methodically stalked and murdered his former girlfriend after first researching whether Illinois has the death penalty. After determining that the state had abolished the death penalty, he drove to the Chicago area, attached a GPS device on the victim's car, and followed her for several days. He sat by her car in her office parking lot and murdered her when she left work. During the murder, he had to stop and reload his gun in the middle of shooting her.[36]

In 2013, in Petaluma, California a man used a smartphone application to track a victim through her cellphone.[37] He tracked her to a friend's house and was arrested when he assaulted her.

Current Legal Recourse When Location Tracking is Used to Harm Victims

Fortunately, stalking is a crime in all 50 states, the District of Columbia, the U.S. Territories, and there is even a Federal stalking law. Unfortunately, many stalking laws do not address the use of location tracking devices or apps. Some judges have interpreted using location tracking software over a period of time as stalking, but the initial installation may not be considered a crime. Crimes that violate the federal stalking and cyber stalking laws are rarely charged, probably due in part to the high burden in the statutory language and the limited resources of the FBI and U.S. Attorneys.

The Electronic Communications Privacy Act (ECPA)[38] prohibits the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices, however it does not cover devices that surreptitiously track location information. Many of the comprehensive Stalking/Spy apps that I have included in my testimony very likely violate ECPA since they manufacture, send, advertise, and promote the use of a surreptitious interception device – and some of their features intercept electronic communications; it's important to note, however, that there are apps that track only GPS location and do not offer eavesdropping capabilities – and are hence not clearly prohibited under federal law.
Unfortunately, I am only aware of one instance of the U.S. Department of Justice indicting a manufacturer of SpyWare.
In August 2005, United States Attorney Carol C. Lam of the Southern District of California and John C. Richter, Acting Assistant Attorney General for the Criminal Division, U.S. Department of Justice, indicted Carlos Enrique Perez-Melara -- the creator and marketer of a spyware program called "Loverspy" - and four others who used Loverspy illegally to break into the victims' computers and illegally intercept the electronic communications of others.[39]

> "Purchasers would then select from a menu an electronic greeting card to send to up to five different victims or email addresses. The purchaser would draft an email sending the card and use a true or fake email address from the sender. Unbeknownst to the victims, once the email greeting card was opened, Loverspy secretly installed itself on their computer. From that point on, all activities on the computer, including emails sent and received, web sites visited, and passwords entered were intercepted, collected and sent to the purchaser directly or through Mr. Perez's computers in San Diego. Loverspy also gave the purchaser the ability to remotely control the victim's computer,

[36] Huffington Post, Dmitry Smirnov Pleads Guilty, Gets Life In Stalking Murder Of Ex-Girlfriend Jitka Vesel. First Posted: 07/23/11 Updated: 09/22/11 www.huffingtonpost.com/2011/07/23/dmitry-smirnov-pleads-gui_n_907839.html

[37] CBS San Francisco and Bay City News Service. Petaluma Man Arrested For Stalking Woman. November 13, 2013 http://sanfrancisco.cbslocal.com/2013/11/13/petaluma-man-arrested-for-stalking-woman/

[38] 18 U.S. Code § 2512 Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

[39] U.S. Department of Justice, Press Release. August 26, 2005 http://www.justice.gov/criminal/cybercrime/press-releases/2005/perezIndict.htm

> including accessing, changing and deleting files, and turning on web-enabled cameras connected to the victim computers. Over 1,000 purchasers from the United States and the rest of the world purchased Loverspy and used it against more than 2,000 victims. Mr. Perez's operations were shut down by a federal search warrant executed in October 2003."[40]

On November 5, 2013, the FBI announced the addition of Mr. Perez to its Cyber's Most Wanted List and is seeking information from the public regarding his whereabouts.[41] (Mr. Perez fled the country at the time of his indictment.) Mr. Perez was indicted for manufacturing a surreptitious interception device; sending a surreptitious interception device; advertising a surreptitious interception device; advertising and promoting the surreptitious use of an interception device; intercepting electronic communications; disclosing electronic communications; and unauthorized access to a protected computer for financial gain.

Legal Loophole for Location in ECPA

Many location tracking stalking apps that only capture and disclose location would not violate ECPA, since ECPA does not cover location interception alone. This legal loophole allows app and device developers to create products that track and share a victim's location, 24 hours a day, as she goes to the police department to file a report, the courthouse to apply for a protection order, and the undisclosed and highly hidden domestic violence shelter to an abusive individual. More specifically, while ECPA requires user consent before a company shares the contents of that user's communications, the law allows a commercial entity to share a user's location information without his or her consent. As noted above, there are many location tracking "Stalking Apps" that only capture and disclose location, which would not violate ECPA, since ECPA does not cover location interception alone.

III. The Solution

A. Require consent prior to tracking or sharing information

Technology companies that develop location tracking tools or applications that rely on location tracking to improve their functionality can help protect victims by ensuring that the consumer has notice of the location information collected, whether that information is transmitted in real-time, who has access that information, and the length of time for which location information is retained. These concepts are not new – robust notice and truly informed consent has been best practice since the Fair Information Practices were articulated in the 1970s.[42] In 2010, The Wireless Association (CTIA) published industry "*Best Practices and Guidelines for Location Based Services.*"[43] These guidelines "rely on two fundamental principles: user notice and consent."[44]

Survivors of abuse and all users must be informed about how their location information will be used, disclosed, and shared. This process should be prominent, transparent, and easy to understand. As noted in CTIA's *Guidelines*, "Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the Location Based Service (LBS) portion must

[40] Ibid.

[41] U.S. Department of Justice, Press Release. November 5, 2013 http://www.fbi.gov/sandiego/press-releases/2013/fbi-seeks-information-regarding-several-cyber-fugitives

[42] http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

[43] CTIA. *Best Practices and Guidelines for Location Based Service.* Volume 2.0. March 23, 2010. Available at: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf and www.ctia.org/policy-initiatives/voluntary-guidelines/best-practices-and-guidelines-for-location-based-services

[44] Ibid.

be conspicuous."[45] Knowing how and when their location information (via mobile device) is gathered and shared will help empower victims to develop strategies to minimize their vulnerability and determine whether or not it is safe to carry their mobile phone and/or to purchase a new phone that will provide greater privacy and safety.

Users must have the opportunity to actively and meaningfully consent to the use, disclosure, or sharing of their location information. Meaningful consent must be prominent, succinct, and very easy to navigate. "Pre-checked boxes that automatically opt users in to location information disclosure, or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent."[46] Consent is especially critical when the product or application does not require location information in order to function. For example, some mobile internet browsers may retain location information regarding past wireless access points users have accessed. This may allow the device to more quickly access wireless internet in the future when an individual returns to that location. However, this is not critical to the functioning of the device. The device can search anew for internet access each time the user visits that physical location. While this will take more time, some consumers would prefer an increased wait time to having the device maintain unencrypted location log files for an unspecified amount of time. This may be especially true for victims of stalking and domestic violence, who have very real concerns about their personal safety.

Consumers can only truly consent when they have been provided with enough information to gain a full understanding of the collection, transmission, and retention practices and policies of the applications and services they use. Again CTIA's *Guidelines* agrees: "All entities involved in the delivery of LBS, including wireless carriers, device manufacturers, operating system developers, application aggregators and storefront providers, should work to educate users about the location capabilities of the devices, systems, and applications they use as well as to inform them of the various privacy protections available."[47] When consumers understand all elements of their devices and applications, they can make fully informed decisions that may enhance the privacy of many users and increase the safety of some especially vulnerable consumers, including battered women and consumers with low literacy and/or limited English proficiency.

B. Location tracking must be transparent and visible to users

Consent is critical, but consent alone is insufficient. It is common for abusers and stalkers to install tracking apps or devices without the knowledge of the victim/user/target of the tracking. Since the device cannot know if the actual user is consenting or if perhaps a stalker consented during a surreptitious install, a reminder that the user's location is being tracked is critically needed.

Relatively simple safeguards can be added to help prevent misuse of the product and unauthorized access to information. For location-based services, this could take the form of periodic text messages, splash notification, or an ever-present icon to notify and remind the user that a tracking application is on the device. It can also take the form of a central transparent place to view all device features and additional applications that are requesting use of your mobile phone's location. The iPhone, for example, lists all applications (e.g. Camera, Maps, Twitter, Yelp, etc.) that want to use location services and provides the user with an easy way to turn the location services on or off for the entire phone or for any individual application.

---

[45] Ibid.
[46] Ibid.
[47] Ibid.

If location tracking technology is being used legitimately to monitor children or employees, there is no need for a "stealth mode" or for it to run invisibly. The reputable family safety and location sharing social products only function with full notice, consent, and visibility. Location tracking technology designed to run in stealth mode is being designed to facilitate stalking and spying. In 2005, the AntiSpyware Coalition, consisting of major anti-spyware companies, software developers, and non-profit groups, created a consensus definition of spyware, which stated that tracking software, done covertly is spying".[48]

Excerpt from the Definitions:[49]

The table below lists some technologies that have been used to harm or annoy computer users. It is important to note that with proper notice, consent, and control some of these same technologies can provide important benefits: tracking can be used for personalization, advertisement display can subsidize the cost of a product or service, monitoring tools can help parents keep their children safe online, and remote control features can allow support professionals to remotely diagnose problems.

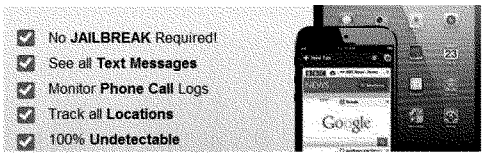
For example, the underlying technology that enables a keylogger is Tracking Software. Tracking Software can both harm and help a user. When a keylogger is installed and executed covertly, it is spying. On the other hand, a keylogger can be used for legitimate purposes with clear consent, such as letting an IT help desk remotely assist a user in problem diagnosis. An underlying technology typically becomes unwanted when it is implemented in a way that provides no benefit to -- or actively harms -- authorized users.

Underlying Technology	Description of Underlying Technology	Why the Underlying Technology May Be Wanted	Why the Underlying Technology May Be Unwanted	Common Terms for Well- Known Unwanted Varieties
Tracking Software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.	May be used for legitimate monitoring: e.g. by parents or companies. May be a necessary component of adware that is linked to wanted software. May allow customization	**Done covertly, tracking is spying** May collect personal information that can be shared widely or stolen, resulting in fraud or ID theft. Can be used in the commission of other crimes, including domestic violence and stalking. Can slow machine down May be associated with security risks and/or loss of data.	Spyware (narrow)* Snoopware Unauthorized Keylogger Unauthorized Screen Scraper

"Emma" fled to Minnesota from the other side of the country, seeking safety. Her stalker found her anyway, shattering her sense of safety. From 1,400 miles away, he would text message her that he knew exactly where she was and who she was with. She couldn't figure out how he knew where she was. Then, on a day she took a trip outside of the rural Minnesota County where she lived, he showed up out of nowhere. She was terrified. Soon after, he moved to Minnesota. The stalking got worse. Emma and her advocate went to her cellphone carrier and law enforcement. Everyone said: you've got GPS tracking spyware on your phone – that's how he knows your every move. But the police didn't have the technology and training to examine the phone or remove the stalking app. ~ Advocate in Minnesota

[48] Anti-Spyware Coalition agrees spyware definition. SC Magazine. November 3, 2005 www.scmagazine.com/anti-spyware-coalition-agrees-spyware-definition/article/32584/

[49] http://www.antispywarecoalition.org/documents/definitions.htm



C. Criminalize the operation, sale, and marketing of technologies whose primary purpose is to surreptitiously track someone's location and facilitate a crime

It is currently a crime to manufacture, distribute, possess, and advertise electronic communication intercepting devices.[50] It is past time to also criminalize intercepting tracking location in addition to electronic communication.

Enactment of new federal and state criminal statutes criminalizing bad acts that misuse location technologies will have several positive effects. First, enacting new criminal statutes will empower law enforcement officials to target emerging, technology-aided forms of stalking or abuse and focus the criminal justice system's efforts towards penalizing bad acts. This may be especially valuable in the case of stalking or domestic violence where it is often the case that a series of escalating behaviors are a prelude to an ultimately tragic event. Equipping law enforcement with new statutes and new, potent penalties may allow for interventions before tragedies occur. Second, the enactment of these statutes may give victims and their lawyers and advocates new opportunities to seek out prosecutions, thereby empowering individuals that otherwise may feel powerless. Holding abusers and stalkers accountable will have a significant, beneficial effect for some victims and may help deter escalating abuse or break the cycle of abuse they are suffering. Third, it will help eliminate marketing of technologies that are designed to facilitate stalking and similar abuses.

> HelloSpy is the most powerful mobile phone spy and tracking software that lets you monitor ALL the activities of any iPhone or Android phone. HelloSpy is super easy to install on the phone you want to monitor. It starts uploading the monitored phone's usage information and its exact location instantly which can be viewed by logging in to your HelloSpy user area from any computer(or smartphone) in the world within minutes. This state-of-the-art application works in stealth mode which means that it will never be found on the target cell phone.

D. Allow law enforcement to seize the proceeds of those sales to fund anti-stalking efforts

No one should profit from encouraging or enabling criminal acts, and stalking app and device developers are creating and selling crime-facilitating products with abandon. Federal law (18 U.S.C. § 2513) provides that entities who violate the prohibition on wiretapping (18 U.S.C. § 2511) and the prohibition on making a device whose primary purpose is wiretapping (18 U.S.C. § 2512) can have the devices used to commit those violations forfeited. Funds seized from companies promoting stalking and abuse should go to support prevention, awareness, and training to help end stalking and abuse.

[50] 18 U.S. Code § 2512 Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

E. Allow individuals an enforcement option through a VERY modest private right of action

The proposed protections for victims will be of little use without effective enforcement mechanisms The Attorney General has limited resources and not every division can prioritize resources for prosecution. Individual victims must be able to obtain recourse. It is also in the interest of public safety for the entire community, not just for an individual stalking victim, to hold accountable developers who willfully and knowing develop and market apps and devices to facilitate crime.

Since the penalties proposed in the bill are capped globally at $1 million for accidental acts or omissions, and $2 million for intentional or willful violations, these amounts would be de minimis to any large reputable company; however, the amounts could be a vital incentive to counter the potential profits an unscrupulous developer may earn by marketing and selling to stalkers.

Please note that many small businesses carry liability insurance that would likely cover non-willful violations. Small businesses are typically required to carry insurance if they want to take out a lease or loan, and per some contracts.

F. Require the federal government to gather more information about GPS stalking, facilitate reporting of GPS stalking

NNEDV supports gathering more information and statistics while recognizing the staggering financial cost to doing comprehensive national supplemental studies. In early 2004, staff from the U.S. Department of Justice Office (DOJ) Office on Violence Women (OVW) worked with the DOJ Bureau of Justice Statistics (BJS) to develop a special survey on stalking. At the time, the most recent data were nearly 10 years old and there was a critical need for more detailed information about victims of stalking, offenders who commit stalking, victim interaction with the criminal justice system, and the monetary cost of stalking to victims and society in general. OVW and BJS agreed to work in partnership to develop a "stalking supplement" to the National Crime Victimization Survey (NCVS).

In the absence of a comprehensive national study, many smaller studies and surveys have shown an increase in the incidence of technology misuses corresponding to the increase by the broader community of technology use.

G. Require the federal government to prioritize funding for GPS stalking prevention, awareness, and detection efforts

20% of stalking victims stated the police took no action when contacted.[51]

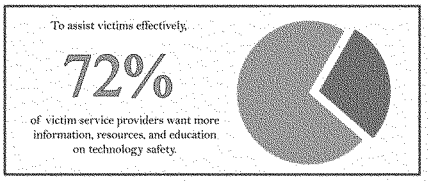
NNEDV has trained over 65,000 police, prosecutors, victim advocates, judges, and other professionals in the past 12 years on the safe use and misuse of technology. Given the high rate of turn-over in these demanding and underpaid professions, ongoing technology training is needed – even in communities that were trained recently. NNEDV is able to accept one training invitation for every two-three training requests that we have to turn down. Every ballroom filled with officers and advocates equals thousands of victims who will have a trained support system that understands location privacy and technology stalking. Unfortunately the demand for training far exceeds the

> "Spyware that can easily be installed on mobile phones is often used by abusers and stalkers to track or contact women who have filed protection orders against them. Police need to be aware of these technologies and the role they can play in stalking and domestic violence situations." Orvena Gregory, Second Chief, Sac and Fox Nation (Oklahoma)

[51] Center for Policy Research, Stalking in America, July 1997

funded training resources. NNEDV's Safety Net Team could double our staff from two full-time trainers to 4 full-time trainers and still need to turn down far too many training requests.

Training is needed and has been requested by officers and advocates in all states, U.S. Territories, and Tribal communities. A 2012 survey found that 72% of victim service providers want more training and resources on technology stalking and safety.[52]



H. Enact parallel state and Tribal laws to allow local, state, and Tribal level enforcement

NNEDV is hopeful that the Location Privacy Protection Act of 2014 will become a model for state legislatures and for NNEDV's member state domestic violence coalitions to develop state complementary laws. Such state laws could expand the enforcement from federal to state law enforcement since the overwhelming majority of stalking and domestic violence investigations are completed by local police and corresponding charges are filed by local prosecutors.

IV. Conclusion

NNEDV supports innovation and has seen countless positive ways that technology, when developed thoughtfully, can increase the safety and support for survivors of abuse and stalking. We are proud of the close working relationship that we have with technologists and we thank Verizon, Google, Facebook, Apple, and the Application Developers Alliance for consistently working with us to increase survivor safety. The Location Privacy Protection Act of 2014 will narrowly impact a handful of bad actors that design or operate products created and sold to facilitate terrifying crimes. Senator Franken, thank you for your tireless and ongoing efforts to end violence against women. Thank you to Ranking Member Flake and the entire committee for your long support of VAWA and these important location protections for survivors.

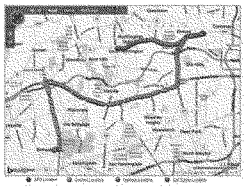
> After getting a protection order "Beth" began seeing her abuser everywhere. As a nurse, her scheduled days to work were variable, and she did not always go straight home, so she really didn't feel her whereabouts were "extremely predictable." Beth took her phone for service, and explained everything to them. The phone had applications running on it that they were unfamiliar with. Unfortunately Beth's reports of stalking were not believed. It took her ex brutally bludgeoning her almost death for them to take her seriously. Beth survived that attack. Her ex was convicted of 1st degree attempted murder and is now serving a decades-long sentence. ~ Advocate in Minnesota

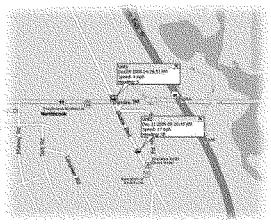
[52] NNEDV, "New Survey: Technology Abuse & Experiences of Survivors and Victim Service Agencies," www.ovc.gov/news/grantees.html and http://techsafety.org/blog/2014/4/29/new-survey-technology-abuse-experiences-of-survivors-and-victim-services (data collected in 2012)

A Sampling of Tracking Apps and Devices Marketed to Stalkers

A Sampling of Features and Different Spying and Stalking Devices

Question: Is the application invisible?
Answer: mSpy works in stealth mode. It does not display any icons and appears on the device application database under different names (system processes), which leaves virtually no chance for the user to identify this software. Moreover, there are neither logs stored on the target device nor pop-up messages ever showing up on the main screen.



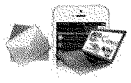


Android Spy Software
100% Undetectable - Monitor Android Devices Remotely

Monitor iPhone Without a Jailbreak!
View Text Messages, iMessages, Locations and more!

Spy On Email
The user can easily go through all the emails that get handled via the target cell phone. So if you doubt that your employee might be carrying the crucial information out via emails. Click below for more features

View Incoming / Outgoing E-mails



Track GPS Location
With the inbuilt GPS device, the GPS Software of Imobitapy efficiently traces and records all the GPS locations of the monitored cell phone. Click below to view features.

View current GPS location

Monitor Internet Activities
This feature will enable the user to get through all the websites that the monitored cell phone user has browsed. Click below for more features

URL Tracking

PREPARED STATEMENT OF CHAIRMAN LEAHY

Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary,
Hearing on "The Location Privacy Protection Act of 2014"
Subcommittee on Privacy, Technology and the Law
June 4, 2014

Today, the Subcommittee on Privacy, Technology and the Law will discuss Senator Franken's Location Privacy Protection Act, which he reintroduced earlier this year. I commend the Subcommittee's Chairman for holding this important hearing and for his work on consumer privacy issues.

With the explosion of smart technologies and mobile applications, now commonly referred to as "apps," American consumers face threats to privacy now like never before. Many of us carry smart devices, such as smartphones and tablets, at all times and use them for anything from navigational and social networking purposes to shopping and playing games. While this technology has brought many new benefits to consumers, it has also raised troubling questions and presented new challenges for how to protect individuals' privacy.

Over the past year, Congress has spent a good deal of time debating important questions relating to government collection of Americans' data. But I also remain concerned about reports that more and more mobile apps are collecting, storing, and tracking location data for their own commercial purposes without adequately informing users, and that this location data can too easily be misused to commit crimes – including cyber-stalking and domestic violence. Last year, the Leahy-Crapo Violence Against Women Reauthorization Act expanded the definition of stalking to include threats or harassment by any electronic means. This important change strengthens protections for victims and gives law enforcement the ability to bring cyberstalkers to justice. Senator Franken's bill builds on that foundation by addressing the growing problem of "stalking apps," which permit abusers to track their victims' location without their knowledge.

As smart technologies become an ever larger part of our daily lives, the widespread commercial collection of geolocation data will continue to grow. Americans deserve to have more control over this information, and Congress must keep a watchful eye on how this data is collected and used. I look forward to learning the witnesses' perspective on this important issue.

#####

PREPARED STATEMENT OF CHAIRMAN FRANKEN

Opening Statement of Chairman Al Franken (D-MN)
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
"The Location Privacy Protection Act of 2014"
June 4, 2014

This hearing will be called to order. Welcome to the Senate Judiciary Subcommittee on Privacy, Technology and the Law. This is a hearing on my bill to protect sensitive location information, the Location Privacy Protection Act of 2014.

Three years ago, I held a hearing to look at how our laws were protecting the location information generated by smartphones, cellphones and tablets. The first group I heard from was the Minnesota Coalition for Battered Women. They told me that across Minnesota, victims were being followed through so-called "stalking apps" specifically designed to help stalkers secretly track their victims.

I started investigating these stalking apps. Let me read you from some of their websites.

Here's one called SPYERA – quote: "Most of the time if you think your spouse is being unfaithful, you are right." "[SPYERA] will be your spy in their pocket." "[Y]ou will need to sneak your spouse's phone and download it to their phone." "After the software is downloaded… you will be able to see where they are geographically. If your husband is in two counties over from where you live, SPYERA will tell you that."

Here's another - quote: "FlexiSPY gives you total control of your partner's phone without them knowing it… See exactly where they are, or were, at any given date and time." Unquote.

And here's another quote that's since been taken down – quote: "Worried about your spouse cheating?" "Track EVERY text, EVERY call and EVERY Move They make Using our EASY Cell Phone Spy Software."

These apps can be found online in minutes. And abusers find them and use them to stalk thousands of women around the country.

The Minnesota Coalition for Battered Women submitted testimony about a northern Minnesota woman who was the victim of domestic violence – and the victim of one of these stalking apps. This victim had decided to get help. And so she went to a domestic violence program located in a county building. She got to the building, and within five minutes, she got a text from her abuser asking her why she was in the county building. The woman was terrified. And so an advocate took her to the courthouse to get a restraining order. As soon as she filed for the order, she got a second text from her abuser asking her why she was at the courthouse, and whether she was getting a restraining order against him.

They later figured out that she was being tracked through a stalking app installed on her phone.

This doesn't just happen in Minnesota. A national study conducted by the National Network to End Domestic Violence found that 72 percent of victim services programs across the country had seen victims who were tracked through a stalking app or a stand-alone GPS device. Without objection, I'll add to the record the accounts of a few other victims.

Here's one from a victim in Illinois. She was living in Kansas with her abuser. She fled to Elgin, Illinois, a town 3 states away. She didn't know that the whole time, her cellphone was transmitting her precise location to her abuser. He drove 700 miles to Elgin. He tracked her to a shelter and then to the home of her friend, where he assaulted her and tried to strangle her.

Here's one from a victim in Scottsdale, Arizona. Her husband and she were going through a divorce. Her husband tracked her for over a month through her cellphone. Eventually, he murdered their two children in a rage.

In most of these cases, the perpetrator was arrested – because it's illegal to stalk someone. But it's not clearly illegal to make and market and sell a stalking app. And so nothing happened to the companies making money off of stalking. Nothing happened to the stalking apps.

My bill would shut down these apps once and for all. It would clearly prohibit making, running, and selling apps and other devices that are designed to help stalkers track their victims. It would let police seize the money these companies make and use that money to actually prevent stalking. My bill will prioritize grants to the organizations that train and raise awareness around GPS stalking. And it would make the Department of Justice get up-to-date statistics on GPS stalking. That's a big deal, because the latest statistics we have from DOJ are from 2006 – and at that point they estimated over 25,000 people were being GPS stalked annually.

But my bill doesn't protect just victims of stalking. It protects everyone who uses a smartphone, an in-car navigation device, or any mobile device connected to the Internet. My bill makes sure that if a company wants to get your location or give it out to others, they need to get your permission first.

I think that we all have a fundamental right to privacy: a right to control who gets your sensitive information, and with whom they share it. Someone who has a record of your location doesn't just know where you live. They know where you work and where you drop your kids off at school. They know church you attend, and the doctors you visit.

Location information is extremely sensitive. But it's not being protected the way it should be. In 2010, the *Wall Street Journal* found that half of the most popular apps were collecting their users' location information and then sending it to third parties, usually without permission.

Since then, some of the most popular apps in the country have been found disclosing their users' precise location to third parties without their permission. And it's not just apps. The Nissan Leaf's on-board computer was found sending drivers' locations to third party websites. OnStar threatened to track its users even after they cancelled their service; they only stopped when I and other Senators called them out on this. And a whole new industry has grown up

around tracking the movements of people going shopping – without their permission, and sometimes when they don't even enter a store.

The fact is most of this is totally legal. With only a few exceptions, if a company gets your location information over the Internet, they are free to give it to almost anyone they want.

My bill closes these loopholes. If a company wants to collect or share your location, it has to get your permission first and put up a post online saying what the company is doing with your data. Once a company is tracking you, it has to be transparent – or else it has to send you a reminder that you're being tracked.

Those requirements apply only to the first company getting location information from your device. For any other company getting large amounts of location data, all they have to do us put up a post online explaining what they're doing with that data.

That's it. These rules are built on existing industry best practices, and they have exceptions for emergencies, theft prevention, and parents tracking their kids. The bill is backed by the leading anti-domestic violence and consumer groups. Without objection, I'll add letters to the record from the Minnesota Coalition for Battered Women, the National Center for Victims of Crime, the National Women's Law Center, the Online Trust Alliance, and Consumers Union – all in support of my bill.

This is bill is just common sense.

Before I turn it over to my friend the Ranking Member, I want to make one thing clear. Location-based services are terrific. I use them all the time when I drive across Minnesota. They save time and money, and they save lives. Ninety-nine percent of companies that get your location information are good, legitimate companies.

And so I've already taken into account many of the industry concerns that I heard when we debated this bill last Congress: I've capped liability, I've made compliance easier. But if folks still have issues with the bill, then I want to address them.

With that, I'll turn it over to Senator Flake.

QUESTIONS SUBMITTED TO ROBERT D. ATKINSON BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 11, 2014

Robert Atkinson

1. During the hearing there was considerable discussion of stalking apps but also legitimate tracking apps. Could you explain what you think the difference is between a stalking app and a tracking app?

    a. In addition, at a technical level, is it possible to distinguish between apps that track individuals imperceptibly for legitimate reasons versus illegitimate reasons?

2. Would it be useful in the legislation to distinguish between apps that can be used to stalk individuals and those that use geo-location data for other purposes?

3. In requiring the 24 hour to 7 day notice, the bill applies this requirement to a "covered entity that initially collects geolocation information from an electronic communications device in a manner that the covered entity has reason to believe is imperceptible to the individual using the electronic communications device..." From a technical perspective, how do you define "imperceptible?"

QUESTIONS SUBMITTED TO LUIGI MASTRIA BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 11, 2014

Lou Mastria

1. In your testimony, you stated that the Digital Advertising Alliance (DAA)'s self-regulatory program is backed by enforcement mechanisms. How is this program enforced?

    a. What penalties, sanctions, or other actions are performed to bring companies into compliance with the guidelines?

2. What tools and/or programs does the DAA offer to consumers to provide transparency and control to consumers regarding the data collection?

    a. Do consumers use these tools, and how do they impact the growth of the Internet economy?

QUESTIONS SUBMITTED TO MARK L. GOLDSTEIN BY SENATOR FRANKEN

Written Questions of Senator Al Franken
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 11, 2014

Mark Goldstein

1. Mr. GOLDSTEIN, to me, one of your most interesting findings was the lack of transparency around the downstream sharing of location data. According to your report, app companies are not telling users the third party companies that they're turning around and sharing that data with. Mr. GOLDSTEIN, right now, is there any way for consumers to find out who exactly is getting their location data from the original app that collected it?

QUESTIONS SUBMITTED TO JESSICA RICH BY SENATOR FRANKEN

Written Questions of Senator Al Franken
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 11, 2014

Jessica Rich

1. Ms. RICH, the FTC has issued best practices for app developers. One of the key best practices you have is that app developers should always get affirmative express consent before collecting or sharing sensitive information like geolocation data. It's not enough for apps to do it and then let users opt-out.

My bill also sets up an opt-in rule for collection or sharing of location data. Why did you set this standard where you did – and is there precedent for it?

RESPONSES OF ROBERT D. ATKINSON TO QUESTIONS SUBMITTED BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 11, 2014

Robert Atkinson

1. During the hearing there was considerable discussion of stalking apps but also legitimate tracking apps. Could you explain what you think the difference is between a stalking app and a tracking app?

    a. In addition, at a technical level, is it possible to distinguish between apps that track individuals imperceptibly for legitimate reasons versus illegitimate reasons?

    "Stalking apps" covertly track and report a user's location to another individual without the user's permission and in violation of the laws on stalking. Legitimate tracking apps, such as those designed to monitor the location of a stolen device, child, or employee, similarly track the location of an individual but do so within the bounds of the law. Similarly, apps such as CarrierIQ monitor mobile devices unobtrusively to improve network performance and diagnose network connectivity issues. At a technical level, there is little to no difference between geolocation apps used to stalk individuals and those used for legitimate purposes. Both types of apps collect, transmit, and store location information about the user and make it available to others. The principle difference between these apps is in how they are marketed and what the data are used for and in some case in the level of transparency provided to the user.

2. Would it be useful in the legislation to distinguish between apps that can be used to stalk individuals and those that use geo-location data for other purposes?

    Yes. While there is a group of apps that track and report the location of individuals to other users, the vast majority of apps using geolocation data do not share this information with other end-users. For example, many websites personalize their services based on the user's location, such as for news, shopping, and maps. Other sites use the geolocation data to improve the performance of the phone and/or the network. Other apps allow users to share their location information with others, but this is done in the foreground, such as sharing location information on social networks. These apps bear no resemblance to the stalking apps of concern to the committee and so should be excluded from legislation intended to crack down on stalking apps.

3. In requiring the 24 hour to 7 day notice, the bill applies this requirement to a "covered entity that initially collects geolocation information from an electronic communications device in a manner that the covered entity has reason to believe is imperceptible to the individual using the electronic communications device…" From a technical perspective, how do you define "imperceptible?"

Imperceptible does not mean that there is no way to perceive that the electronic device is collecting geolocation information, only that it is being done so in a manner that is very subtle or difficult to perceive. Unfortunately, the bill does not define how a developer might distinguish what is "imperceptible to the individual using the electronic communications device." There are small signals that developers might argue count towards notifying the user. For example, devices collecting and transmitting geolocation data generally use more processing power which means they tend to run a bit hot and consume battery power more quickly than devices that are not doing so. Likely this is not the threshold the authors of the bill had in mind.

While legitimate apps generally do not actively try to obfuscate their activity from the user, some legitimate apps may run in the background without directly alerting the user they are collecting geolocation data so as to minimize unnecessarily bothering the user. But these apps will still appear in if the user checks the list of running processes, especially using a popular task killer app. Would this level of disclosure meet the threshold for being considered imperceptible?

Or developers could rely on an alert from an icon on the mobile device to signal to the user that geolocation data is being collected. How large does such an icon have to be on a mobile device (and does it matter the size of the screen)? Or does it matter if the developer knows that the user has low vision or no vision? If user testing reveals that users do not understand the meaning of their devices geolocation icon, does the developer have to take additional action? And is notification still considered perceptible if it is buried after 20 other notification on the device's screen? In addition, to what extent is the app imperceptible if the installer can turn off notifications?

These are just a sampling of the type of real-world problems that developers might encounter trying to comply with this law. This is yet another reason why if Congress pursues this legislation, it should narrowly target this bill to a small class of apps where the location data can be accessed by the person installing the app on the phone while also providing a more robust definition of "imperceptible"

RESPONSES OF LUIGI MASTRIA TO QUESTIONS SUBMITTED BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014
June 26, 2014

Lou Mastria

1. ***In your testimony, you stated that the Digital Advertising Alliance (DAA)'s self-regulatory program is backed by enforcement mechanisms. How is this program enforced?***

    a. ***What penalties, sanctions, or other actions are performed to bring companies into compliance with the guidelines?***

A key feature of the DAA Self-Regulatory Program is accountability. The DAA's Self-Regulatory Principles ("Principles") are backed by two robust enforcement programs administered by the Council of Better Business Bureaus ("CBBB") under the policy guidance of the Advertising Self-Regulatory Council (ASRC), and by the Direct Marketing Association (DMA) under its *Guidelines for Ethical Business Practice* (collectively, "Accountability Programs"). Accountability under the DAA Principles applies to all companies operating in the advertising ecosystem, not merely "participants" in the DAA Program.

Since this hearing, new enforcement actions were announced. The DAA has, to date, brought 37 publicly announced compliance actions involving brand-name companies and lesser-known names, and the actions have addressed well-known technologies and emerging technologies. These actions have addressed traditional online display advertising, as well as social media. These results demonstrate robust accountability that is responsive and can quickly adapt to emerging business and technology models in the marketplace.

The goal of the DAA Accountability Programs is to identify instances of noncompliance by companies and help those companies come into compliance and build consumer trust through good advertising practices online. While the Accountability Programs do not seek to be punitive, the DAA believes that strong, independent enforcement is essential to successful self-regulation, and therefore, reserves the right to publicly report on instances of noncompliance and report uncorrected violations to the appropriate government agencies.

The CBBB Accountability Program builds on the successful track records of several other ASRC programs that have been in place for decades. These programs feature independent monitoring and public reporting of decisions. They have extremely high voluntary compliance rates. Those companies that fail to comply or refuse to participate in the self-regulatory enforcement process are referred publicly to the appropriate government agency for further review.

The CBBB administers its Interest-Based Advertising Accountability Program under the ASRC self-regulatory policy guidance and procedures. Because of the highly complex, technical and interdependent nature of interest-based advertising, the Accountability Program receives a

weekly privacy dashboard report based on independent data about companies' compliance with various requirements of the Principles. The Accountability Program's technical staff analyzes these data and examines whether there may be a violation of the Principles warranting formal inquiry. The Program also finds potential cases through its own staff monitoring and investigation, by analysis of consumer complaints and reviews of news stories and technical reports from academics and advocacy groups.

Where there is a potential compliance issue, the CBBB initiates formal inquiries and works to ensure the company understands the Principles and voluntarily implements the requirements of the Principles. At the end of the process, the CBBB Accountability Program issues a public decision, which details the nature of the inquiry, the Accountability Program's conclusions, any recommendations for correction, and includes a statement from the company in question regarding its implementation of the recommendations. A press release is also issued.

The DMA's longstanding *Guidelines for Ethical Business Practice* ("*Guidelines*") set out comprehensive standards for marketing practices, which all DMA members must follow as a condition of membership. The DAA Self-Regulatory Principles are incorporated into these *Guidelines*.

The DMA's Ethics Operating Committee ("Committee") examines practices that may violate the *Guidelines*. To date, the *Guidelines* have been applied to hundreds of marketing cases on a variety of issues such as deception, unfair business practices, personal information protection, and online behavioral advertising. The Committee works with both member and non-member companies to gain voluntary cooperation in adhering to the guidelines and to increase good business practices for direct marketers. The Committee receives matters from consumers; member companies; non-members; or, sometimes, consumer protection agencies. Complaints are reviewed against the *Guidelines* and if a potential violation is found to exist, the company is advised on how it can come into full compliance.

Most companies work with the Committee to cease or change the questioned practice. If a member company does not cooperate and the Committee believes there are ongoing *Guidelines* violations, the Committee can recommend that action be taken by the DMA Board of Directors and can make case results public. Board action could include censure, suspension or expulsion from membership, and the Board may also make its actions public. If a non-member or a member company does not cooperate and the Committee believes violations of law may also have occurred, the case is publicly announced and may be referred to federal and/or state law enforcement authorities for review.

The CBBB and DMA programs demonstrate the success of self-regulation and its many benefits, including the ability for the regulatory apparatus to evolve to meet new challenges.

2. ***What tools and/or programs does the DAA offer to consumers to provide transparency and control to consumers regarding the data collection?***

    a. ***Do consumers use these tools, and how do they impact the growth of the Internet economy?***

The DAA Program provides consumers with enhanced transparency around data practices and choice with respect to collection and use of their Internet viewing data while preserving the ability of companies to responsibly deliver services and continue innovating. This approach allows consumers to enjoy the incredibly diverse range of Web sites by preserving the responsible data flows that support these offerings and that fuel our nation's economy.

The DAA Program fosters this approach by providing tools and mechanisms that enable transparency, consumer control, and accountability (as detailed in response to question 1 above).

Transparency. DAA has developed a universal icon ("DAA Icon") deployed by companies that gives consumers transparency and control with respect to interest-based ads. The icon provides consumers with actionable notice that information about their online interests is being gathered to customize the Web ads they see. Clicking the DAA Icon also takes consumers to a centralized choice tool that enables consumers to opt out of this type of advertising by participating companies. The icon is served globally more than *one trillion times each month* on or next to Internet display ads, Web sites, and other digital properties and tools covered by the program. In April 2014, the DAA issued technical specifications that provide companies guidance for providing this transparency tool in mobile web and application environments. This will provide companies and consumers with a consistent, reliable user experience across the multiple screens on which they interact. This will also provide companies a consumer-friendly way to provide enhanced notice and choice outside of the privacy policy.

Furthermore, the DAA Principles call for consumer education. The DAA commissioned a professionally developed advertising campaign to help consumers learn about interest-based advertising and the choices they have with respect to data collection and use. This effort successfully delivered easy to understand videos and messaging to help millions of consumers understand the power at their hands.

Consumer Control. The DAA Program makes available a centralized choice mechanism that unites the opt-out mechanisms provided by more than 115 different third-party advertisers participating in the program. The choice mechanism website offers consumers a "one-click" option to request opt-outs from all participants or allows a user to make choices about opting-out of interest-based advertising from specific companies. Consumers are directed to AboutAds.info not only from DAA Icon-based disclosures on or around ads, but from other forms of website disclosure. In 2012, the DAA also introduced a suite of browser plug-ins to help ensure the persistence of these choices so that consumer preferences are not lost should consumers elect to delete their browser cookies.

Since the DAA Program launch, there have been more than 30 million unique visitors to the DAA program Web sites. *Over three million unique users* have exercised choice using the integrated opt-out mechanism provided at AboutAds.info. Most users visit DAA Program Web sites, learn about their choices, and ultimately choose not to opt-out, showing that once consumers understand how interest-based advertising works, many prefer to receive relevant ads over irrelevant ads. The DAA expects to release versions of this successful consumer choice tool

for mobile environments later this year. These tools will provide consumers control over data collected in mobile web as well as data collected through applications.

Location Data. Of particular relevance to the hearing, the DAA imposes stringent requirements for the collection and use of precise location data for commercial purposes. The DAA program requires consent prior to collection and the provision of an easy to use tool to withdraw such consent. We have required privacy-friendly tools including notice in the download process, notice at first install or other similar measures to ensure that companies are transparent in a consistent manner about data collection and that consumers can make informed choices. To help ensure that both the transparency mechanisms we require are used and that consumer choices are honored, we rely on our accountability programs.

The impact of these tools on the growth of the Internet economy is profound. By offering consumers transparency and control in a way that preserves interest-based advertising, these tools help foster innovation and create jobs. As described in my written testimony, the data-driven marketing economy constitutes a significant share of our GDP, and continues to grow each year.

RESPONSES OF JESSICA RICH TO QUESTIONS SUBMITTED BY SENATOR FRANKEN

Written Questions of Senator Al Franken
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014

Jessica Rich

1. Ms. RICH, the FTC has issued best practices for app developers. One of the key best practices you have is that app developers should always get affirmative express consent before collecting or sharing sensitive information like geolocation data. It's not enough for apps to do it and then let users opt-out.

My bill also sets up an opt-in rule for collection or sharing of location data. Why did you set this standard where you did -- and is there precedent for it?

The Commission supports the LPPA's requirement that covered entities obtain affirmative express consent from consumers before knowingly collecting or disclosing geolocation information. As you note, this approach mirrors guidance in our 2013 staff report on mobile privacy disclosures, in which we discussed the importance of transparency in the mobile space through just-in-time disclosures and obtaining opt-in consent before allowing access to sensitive information like geolocation.[1] Moreover, the FTC's 2012 Privacy Report addressed the heightened privacy concerns presented with the collection and use of sensitive personal information, such as geolocation information, and why robust privacy controls like affirmative express consent are warranted for this kind of information.[2]

Geolocation information is sensitive because it can reveal a consumer's movements in real time and over time. Geolocation may also expose other types of sensitive information, such as health or financial information. For instance, geolocation information can disclose if a consumer has gone to an AIDS clinic or cancer treatment center and how often he or she has gone. It can provide information about where a person lives, works, shops, and goes out to eat. It can disclose a child's route to and from school. As discussed in our Privacy Report, when sensitive information is involved, the likelihood that data misuse could lead to discrimination or other harms is increased. Thus, the Commission has recommended the companies obtain opt-in consent from consumers before collecting sensitive information for either first-party or third-party uses.

The Commission's recommendations are in line with a number of self-regulatory frameworks in which industry agrees that geolocation data is sensitive and should be handled with care.[3] But, inconsistencies in the application of self-regulatory codes can

---

[1] FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013) at 15-16, *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[2] Federal Trade Commission, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) at 59, *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[3] *See, e.g.*, Future of Privacy Forum and Center for Democracy & Technology, *Best Practices for Mobile Application Developers* (July 2012) at 7, *available at* http://www.futureofprivacy.org/best-practices-for-mobile-app-developers (stating that app developers should obtain clear, opt-in permission before

make it challenging for an entity to know exactly what it should do when collecting or using geolocation data. And membership in a self-regulatory body is voluntary. The LPPA provides much-needed rules of the road that can help industry compliance and provide enforcement tools to ensure that consumers are protected.

---

accessing precise location data); Network Advertising Initiative, *2013 NAI Mobile Application Code*, at 2, *available at* http://www.networkadvertising.org/code-enforcement/mobile (mandating that use of precise location data for advertising delivered across apps, based on the preferences or interests of a user, shall require the user's opt-in consent); Direct Marketing Association, *Direct Marketing Association Guidelines for Ethical Business Practice* (May 2011), at 40, *available at* https://thedma.org/wp-content/uploads/DMA-Ethics-Guidelines.pdf (stating that location information may not be shared with third-party marketers unless the consumer has given prior express consent for the disclosure).

RESPONSES OF MARK L. GOLDSTEIN TO QUESTIONS SUBMITTED BY SENATOR FRANKEN

Written Questions of Senator Al Franken
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
The Location Privacy Protection Act of 2014

Mark Goldstein

1. Mr. GOLDSTEIN, to me, one of your most interesting findings was the lack of transparency around the downstream sharing of location data. According to your report, app companies are not telling users the third party companies that they're turning around and sharing that data with. Mr. GOLDSTEIN, right now, is there any way for consumers to find out who exactly is getting their location data from the original app that collected it?

Privacy policies of mobile industry companies we examined for our September 2012 report on Mobile Device Location Data did not state which specific third parties companies may share consumers' location data with. Most of these policies stated the types of third-party companies location data may be shared with, such as application developers and advertisers, and some policies described third parties with vague terms such as "trusted businesses" or "others." Therefore, consumers cannot find out who exactly is getting their location data from these policies. However, we did not evaluate explicitly whether consumers could successfully request such information from companies, or obtain it through other means for either the Mobile Device Location Data report or the In-Car Location-Based Services report.

SUBMISSION FOR THE RECORD

NATIONAL WOMEN'S LAW CENTER
EXPANDING THE POSSIBILITIES

June 3, 2014

Chairman Patrick J. Leahy
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Ranking Member Chuck Grassley
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Location Privacy Protection Act of 2014, S. 2171

Dear Senator Leahy and Ranking Member Grassley,

On behalf of the National Women's Law Center, an organization that for 40 years has worked to expand the possibilities for women and girls in the areas of education and employment, family economic security, and health, we write to express the Center's support for S. 2171, the Location Privacy Protection Act of 2014 (LPPA). We urge you to support the passage of the LPPA to help prevent the abuse of cellphone and smartphone location technology to facilitate sexual harassment and assault – including stalking, domestic violence, and dating violence – against countless American women and girls.

Technology that allows a third party to monitor a smartphone user's location is frighteningly prevalent. In December 2010, an investigation by the *Wall Street Journal* revealed that of the 101 top smartphone apps, nearly half (47) disclosed a user's location to third parties, typically without the user's consent.[1] Too often, this technology is used to stalk and harass women. In August of 2010, a director of a battered women's shelter in San Jose, California told the *Journal* that victims entering the shelter often complain: "He knows where I am all the time, and I can't figure out how he's tracking me." The same article related the account of a woman in Arizona whose husband stalked her through the use of cellphone GPS technology before eventually murdering their two children and shooting himself.[2] In 2011, testimony before the Subcommittee on Privacy, Technology and the Law confirmed that stalking through cellphones and smartphones remains a serious problem.[3]

In January 2009, a report by the Department of Justice based on the National Crime Victimization Survey revealed that approximately 26,000 persons are victims of GPS stalking

[1] Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J., Dec. 17, 2010, *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.
[2] Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL ST. J., Aug. 3, 2010, *available at* http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html.
[3] *See* http://www.franken.senate.gov/files/documents/110510_NNEDV_MCBW_Mobile_Privacy_Testimony.pdf.

annually, including by cell phone. However, because this report was based on 2006 data, this figure likely grossly understates the scope of this type of abuse. In the intervening eight years since 2006, smartphone use has skyrocketed; the Pew Research Center recently reported that in 2014 over half (58%) of U.S. adults have smartphones, up from 35% in 2011.[4] In addition, many victims do not know that these devices are being used by their stalkers, since many of the tracking capabilities and applications available for cell phones and smartphones can be used against victims without their knowledge.

The Location Privacy Protection Act of 2014 will empower law enforcement, victims' advocates and victims themselves to prevent and combat this abuse of geo-location information. Briefly, it will require companies to obtain a customer's consent before collecting his or her data or sharing it with non-governmental third parties. The bill will also raise awareness, help investigations of GPS stalking, and criminalize the development, sale, and/or intentional operation of "stalking apps" to violate federal anti-stalking and domestic violence laws. *This bill does not concern or affect law enforcement location tracking.*

It also provides for the collection of much-needed data—the bill will require the National Institute for Justice, in conjunction with the Office of Violence Against Women, to conduct a study examining the role geo-location technology plays in violence against women. Beyond the information collected about GPS stalking in the U.S. Department of Justice's 2006 Supplemental Victimization Survey—now sorely outdated—federal authorities have little comprehensive information about the ways in which location technology is used in domestic violence, dating violence, sexual assault, and stalking. Such a study will fill that knowledge gap.

******

The abuse of location technology to perpetrate violence against women is pervasive and must be stopped. The Location Privacy Protection Act of 2014 will help to prevent such abuse. We urge you to support the swift passage of this important bill. If you have any questions, please feel free to contact Lara S. Kaufmann at (202) 588-5180 or lkaufmann@nwlc.org.

Sincerely,

Fatima Goss Graves
Vice President for Education and Employment

Lara S. Kaufmann
Senior Counsel & Director of
Education Policy for At-Risk Students

[4] Pew Research Internet Project, Cell Phone and Smartphone Ownership Demographics (2014), *available at* http://www.pewinternet.org/data-trend/mobile/cell-phone-and-smartphone-ownership-demographics/.

SUBMISSION FOR THE RECORD

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

June 11, 2014

The Honorable Al Franken
Chairman
Subcommittee on Privacy,
Technology and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Jeff Flake
Ranking Member
Subcommittee on Privacy,
Technology and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Franken and Ranking Member Flake:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, opposes S. 2171, the "Location Privacy Protection Act of 2014." The Chamber strongly supports the legislation's goal of combating cyberstalking. However, S. 2171 contains commercial privacy provisions in Section 3 that are overly-broad, ignore technical realities, and fail to recognize successful, ongoing self-regulatory programs.

Geolocation data now is commonly used for many purposes, including locating nearby retailers, restaurants, and services; navigating to specific destinations; finding location-specific news, weather, and special offers; authenticating identities; detecting fraud; mitigating retail theft and loss; improving the location of retail displays for consumer convenience; and connecting with family and friends. With the expected growth of the Internet of Things, beneficial uses of geolocation data will continue to increase. These beneficial uses are markedly different than a cyberstalker using location data to threaten, harass, or commit an act of domestic violence or other heinous crime, all of which are already illegal activities.

The Chamber's concerns with S. 2171 include, but are not limited to, the overbroad definition of a covered entity; the obligations of a covered entity; the regulation of information collection instead of use; the imposition of regulations on entities that collect the geolocation information of more than 1,000 electronic communications devices; and the failure to take into account how consent is impacted if several users operate a device at different times. Since many streets run for great lengths, it serves no purpose to use "street name" in the definition of "geolocation information" as there would be no way to know if the individual was downtown or in the suburbs (e.g., Massachusetts Avenue in Washington, DC). Similarly, "street name" is not always applicable in rural areas where streets may have mile markers instead of names.

The Chamber also is troubled that S. 2171 lacks an exemption for information that is de-identified. The Chamber strongly opposes both the limited preemption language that would allow for a patchwork of inconsistent laws to apply in this area as well as the inclusion of a private right of action that would allow the plaintiffs' class action trial bar to bring potentially excessive, duplicative, and spurious litigation under the statute.

To help protect the privacy of mobile users, there are a myriad of existing self-regulatory programs and user-friendly technological solutions. Thus, legislation in this area is simply unnecessary and would clearly harm innovation, including development of the privacy-enhancing efforts that policymakers seek to foster.

The wireless marketplace is a vibrant, competitive, and consumer-driven environment. Thus, the Chamber is disappointed that S. 2171 associates permissible commercial location information with the criminal use of this data to cause harm or risk to the individual. Therefore, the Chamber opposes S. 2171 in its current form because it would create enormous regulatory uncertainty, stifle innovation, deter private-sector investment, and jeopardize the tremendous growth in wireless applications, services, and devices that has benefited both businesses and consumers. However, the Chamber looks forward to continued discussions with you, your subcommittee colleagues, and your staff on how best to target and combat cyberstalking.

Sincerely,

R. Bruce Josten

cc: Members of the Subcommittee on Privacy, Technology and the Law

SUBMISSION FOR THE RECORD

ConsumersUnion
POLICY & ACTION FROM CONSUMER REPORTS

June 3, 2014

The Honorable Al Franken, Chairman
The Honorable Jeff Flake, Ranking Member
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Franken and Senator Flake:

Consumers Union, the public policy and advocacy division of Consumer Reports, urges support for the Location Privacy Protection Act of 2014 (S. 2171). This bill, introduced by Chairman Franken and cosponsored by Senators Coons, Durbin, Blumenthal, and Warren, would require mobile device manufacturers, wireless service providers, data brokers, and other companies to obtain consumer consent before collecting, storing, and sharing personally identifiable geo-location information.

A 2013 Consumer Reports nationally representative survey of consumers found that 76 percent strongly agreed that companies who collect data about consumers' locations should be legally required to get their permission first. Some smartphone users told us they or a member of their household had been harassed or harmed after someone had used location tracking to pinpoint their whereabouts. In a 2012 survey, we found 65 percent of smartphone users were very concerned about apps that could access their location, contacts, photos, and other personal data without their permission.

We support efforts to give consumers the power to choose whether or not their mobile devices collect and share their location information, and with whom. We believe that the approach adopted in S. 2171 is practical and effective. With exceptions for emergency situations, companies should not be permitted to obtain a consumer's geo-location information, or to share that information with third parties, without the consumer's express consent.

We urge the Committee to move forward on this important issue. We look forward to working with you to ensure that consumer location privacy is protected.

Sincerely,

George Slover
Senior Policy Counsel
Consumers Union

cc: Members, Senate Judiciary Committee

SUBMISSION FOR THE RECORD

Interactive Advertising Bureau
116 E. 27th St. 7th Floor
New York, New York 10016
212.380.4700

June 4, 2014

The Honorable Al Franken
Chairman, Senate Judiciary Subcommittee on Privacy, Technology and Law
223 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Jeff Flake
Ranking Member, Senate Judiciary Subcommittee on Privacy, Technology and Law
153 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Franken and Ranking Member Flake –

I am writing to express the IAB's concerns with S. 2171, the Location Privacy Protection Act. The Interactive Advertising Bureau (IAB) is the leading trade association for the more than 600 media and technology companies that serve and sell digital advertising. While only a small share of the overall $43 billion industry today, mobile advertising in the United States is rapidly growing and totaled $7.1 billion during FY 2013, a 110% increase from the prior year total of $3.4 billion. A share of that growth is attributable to the explosion of location based services unique to consumers' mobile behavior.

The IAB takes consumer privacy very seriously. IAB serves as the Chair of the Board of Directors at the Digital Advertising Alliance (DAA) – the independent, regulatory arm of the industry. The DAA began offering real notice and choice to consumers about data collected for advertising in 2010, expanded the program to include all data collection and strict prohibitions on specifics uses in 2011, and again expanded the program to include mobile applications, and consent to collect precise geo-location data and personal directory data in 2013. The DAA has been recognized by the White House, the Federal Trade Commission, and the Department of Commerce as an example of successful self-regulation. IAB's commitment to the program extends to our member companies, who must publicly adhere to the program as a condition of membership.

IAB is concerned with the bill's conflation of legitimate commercial uses of data that deliver concrete benefit to consumers, with that of abusive criminal behavior. The misappropriation of a user's data for criminal activity is distinctly different from the legitimate commercial practices that consumers have come to expect and value; and, is responsible for much of the free or low-cost digital services and applications we enjoy today.

For example, the definition of geolocation information is very broad; and, would sweep in location data that cannot identify an individual or device with specificity. This broad definition is appropriate to address criminal uses where a broad-based location data point still presents great harm to an identifiable victim; while, anonymous, general location data for marketing purposes such as couponing or promotion of local small business is not identifiable and does not pose the same risks as criminal abuses. Furthermore, the definition does not exempt data collection requested by the user, and necessary to provide a service such as a mapping application or GPS device, which is likely to result in added confusion.

The breadth of data covered by this definition is further compounded by the consent requirements. Prohibition on collection or disclosure of geolocation information without express informed consent is tied to the "individual using the device" rather than the owner of the device or the settings on the device. This significantly hinders the use of devices with multiple users, such as tablets, requiring separate consent from each user each time the device changes hands.

Friction is the greatest enemy to the consumer experience, and a company's success in the marketplace. When multiple permission and disclosure screens stand between the consumer and the content they seek, the consumer does not become more educated about data collection practices, they become frustrated.

Innovation and consumer privacy are not competing interests. In fact, consumer privacy is one of the leading areas of innovation evidenced by the proliferation of services like Whisper, Snapchat, Line, and Tango; and, by leading platforms like iOS and Android competing on granular privacy controls for consumers.

In the rapidly evolving mobile technological environment, industry is continuously adapting to new technologies and innovation in the marketplace to meet consumer needs and preferences. Current industry practice is to acquire consent to collect location data from mobile devices. S. 2171, however, would codify current practice, creating a disincentive for companies to develop new or innovative means for transparency and consumer control over data collection practices. Self-regulation allows industry to pivot as the marketplace changes – the DAA has updated its code of conduct twice in less than two years.

The most recent update to the self-regulatory program, the application of self-regulatory principles to the mobile environment, was released in July 2013 and implementation begins this year. We respectfully ask the Committee to consider the complicated legal regime created by applying criminal standards to commercial regulation; and, to allow the DAA the opportunity to build on its great success by implementing and enforcing the application of self-regulatory principles to the mobile environment.

Respectfully,

/s

Mike Zaneis
EVP & General Counsel
Interactive Advertising Bureau

SUBMISSION FOR THE RECORD

June 4, 2014

The Honorable Al Franken, Chairman
Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

RE: S. 2171, the "Location Privacy Protection Act of 2014"

Dear Chairman Franken:

MAPPS (www.mapps.org), the only national association exclusively comprised of private sector firms in the remote sensing, spatial data and geographic information systems field in the United States, commends your effort in holding today's hearing covering the role of technology advances while protecting consumer privacy. The MAPPS membership spans the entire spectrum of the geospatial community, including Member Firms engaged in satellite and airborne remote sensing, surveying, photogrammetry, aerial photography, LIDAR, hydrography, bathymetry, charting, aerial and satellite image processing, GPS, and GIS data collection and conversion services. MAPPS also includes Associate Member Firms, which are companies that provide hardware, software, products and services to the geospatial profession in the United States and other firms from around the world.

Introduced in March 2014, S. 2171 would amend the Electronic Communications Privacy Act to require that companies obtain individuals' permission before collecting location data from their smartphones, tablets, or in-car navigation devices, and before sharing such information with others. The bill would also ban the development, operation and sale of GPS stalking applications and would allow law enforcement to seize the proceeds of those sales to fund anti-stalking efforts.

S. 2171 is an improvement over previously introduced legislation on this topic, inasmuch as it defines the term "geolocation information". Section 3 of S. 2171 defines "geolocation information" to mean any information that is not the contents of a communication; is in whole or in part generated by or derived from the operation or use of an electronic communications device; and is sufficient to *identify the street name* and name of the city or town in which the device is located; and does not include the Internet protocol address or the home, business, or billing address of the individual, or any component parts of such addresses. In addition, Section 3 of S. 2171 defines "geolocation information service"' to mean the provision of a *global positioning service* or *other mapping, locational, or directional information service*.

MAPPS has been deeply concerned that previous bills in Congress have used the term "geolocation" without defining it. Moreover, on December 1, 2010, the Federal Trade Commission (FTC) issued a draft report, *Protecting Consumer Privacy in an Era of Rapid Change*, using the term without definition.

John M. Palatiello, Executive Director
1856 Old Reston Avenue, Suite 205, Reston, Virginia 20190
(703) 787-6996 info@mapps.org www.mapps.org

The mapping, geographic information systems and geospatial community is deeply concerned that legislation and the FTC report would result in a serious threat to our legitimate business interests, and the clients we serve. The FTC report was very broad in its application. Ostensibly, the report was targeted at internet-based cyber tracking of personal data. However, through the use of terminology without definition, and a failure of the report to limit its scope to specific problem areas, the restrictions suggested in the report would hamper the ability of firms, agencies and organizations to collect, use, share, or apply geospatial data.

Similar to the our original concerns for the FTC proposal, MAPPS also respectfully urges the Senate to use extreme caution and not enact any enforcement or broad regulation that would have a harmful affect on the broad private geospatial community.

Pages 74-75 of the 2010 FTC Preliminary Staff Report stated, "Moreover, staff notes that both sensitive information and sensitive users may require additional protection through enhanced consent. The Commission staff has supported affirmative express consent where companies collect sensitive information for online behavioral advertising and continues to believe that certain types of sensitive information warrant special protection, such as information about children, financial and medical information, and precise geolocation data. Thus, before any of this data is collected, used, or shared, staff believes that companies should seek affirmative express consent. Staff requests input on the scope of sensitive information and users and the most effective means of achieving affirmative consent in these contexts."

Specifically, MAPPS is concerned that such FTC regulation or Federal legislation, which inexactly uses and regulates the term "precise geolocation data", would result in serious and harmful unintended consequences for consumers, geospatial firms, and government programs our member firms serve. The use of the term "geolocation" or other terminology relevant to geospatial activities, as it is used in current or possible future FTC regulation or Federal legislation, could thwart legitimate and desireable business activities; deny consumers the products, technologies and services they are demanding in the marketplace; and impose a significant new liability on our members.

On one hand, the term could mean actual street/house address or on the other hand, the actual location of the individual at any given time, i.e. location provided by cell phone triangulation or some other method. If the geolocation refers to a person's name and address being private, then it is inconsistent with virtually every "open records" law in the United States, and could potentially shut down the nation's commercial aerial and remote sensing satellite market and prevent our member firms from collecting, hosting or distributing ownership information.

Page 5 of the 2010 FTC report stated "Companies should not have to seek consent, for example, to share your address with a shipping company to deliver the product you ordered." We believe similar geospatial data should also be excluded from having to be subjected to consent or waivers.

Page 1 of the 2010 FTC questions for comments asked "Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?" We believe geospatial firms' precise geolocation activities should be excluded. Failure to do so would thwart some common, justifiable, and emerging uses of geospatial data for emergency response/post disaster remediation, insurance, environmental protection, E-911 & ambulance services, fleet management broadband mapping, home security, navigation, mortgage foreclosure monitoring/early warning system, and others. Moreover, many geospatial activities, technologies, and applications development could be deemed illegal. For example, it would be impractical, if not impossible, for our member firms to obtain prior approval or consent from individual citizens prior to acquiring or applying data such as satellite imagery, aerial photography, or parcel, address, or transportation data. FTC regulation or a Federal law of this nature would effectively ban our member firms, or their clients, from important value-added, integration and application activities.

For the purposes of the regulations and privacy efforts currently under consideration by the FTC and or under the breadth of S. 2171, MAPPS respectfully submits the following proposed exclusion definition to provide what the

terms "precise geolocation data", "geolocation information" or "geolocation information services do NOT include, and thus is exempt from the scope of such regulation or legislation, such as S. 2171:

> (a) Any information about the location and shape of, and the relationships among, geographic features, including remotely sensed and map data;
> (b) Any graphical or digital data depicting natural or manmade physical features, phenomena, or boundaries of the earth and any information related thereto, including surveys, maps, charts, remote sensing data, and images;
> (c) Collection, storage, retrieval, or dissemination of graphical or digital data to depict natural or manmade physical features, phenomena, or boundaries of the earth and any information related to such data, including any such data that comprises a survey, map, chart, geographic information system, remotely sensed image or data, or an aerial photograph by surveyors, photogrammetrists, hydrographers, geodesists, cartographers, or other such mapping and geospatial professionals; and
> (d) Data originating from commercial satellite systems licensed to operate by the U.S. government, global positioning systems, geographic information systems, and airborne or terrestrial mapping equipment.

Page 36 of the 2010 FTC report stated "The presentation outlined the virtually ubiquitous collection of consumer data that occurs in multiple contexts and at numerous points throughout a given day – for instance, when consumers browse websites, purchase items with payment cards, or use a geolocation application on a mobile device. In addition, the presentation depicted how companies that collect data through such activities share the data with multiple entities, including affiliated companies, as well as third parties that are many layers removed from, and typically do not interact with, consumers."

The geospatial community is one of the fastest growing in the marketplace. It has been identified by the U.S. Department of Labor as one of the "high growth" sectors of the U.S. workforce. There are numerous legitimate geospatial applications, in a rapidly growing market, that fit the aforementioned scenario. We are concerned that unintended consequences of such FTC regulation or Federal legislation will stymie economic growth, job creation, and introduction of new consumer products enabled by geospatial technologies.

Page 10 of the 2010 FTC report stated, "Some of these practices, such as where a retailer collects a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consent for them is inferred. Others are sufficiently accepted – or necessary for public policy reasons – that companies need not request consent to engage in them." A December 1, 2010 FTC news release stated, "The report adds that, to simplify choice for both consumers and businesses, companies should not have to seek consent for certain commonly accepted practices." In addition, pages 66-67 of the report noted, "Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment. Legal compliance and public purpose: Search engines, mobile applications, and pawn shops share their customer data with law enforcement agencies in response to subpoenas. A business reports a consumer's delinquent account to a credit bureau."

The geospatial activities described in the aforementioned exemption language is consistent with these scenarios and thus, such activities should also be exempt from Federal legislation.

Many states define a number of geospatial or geolocation activities as the practice of professional surveying. Therefore, practitioners are licensed and regulated by the government via state licensing boards. Consumers are already protected.

Moreover, commercial satellite remote sensing firms are licensed to operate by the Federal Government (Department of Commerce). Therefore, there are already statutory standards for such individuals and firms, and the public health, welfare and safety, as well as national interests are already protected by a governmental authority. Further regulation is unnecessary, and would create conflict and confusion among such regulatory schemes. Finally, any such Federal

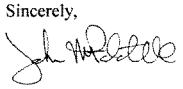
legislation could put U.S. companies at a significant and insurmountable competitive disadvantage against foreign firms that may not be covered by that regulation, or for which enforcement would be impractical.

In conclusion, just as MAPPS urged the FTC to either remove any reference to "precise geolocation data", more specifically and exactly define the term; and/or include the exemption we have suggested herein; and given S. 2171 does define 'geolocation information' and 'geolocation information service', we would also encourage your bill to include the exemption we have suggested herein.

We look forward to working with you to provide the necessary and desirable privacy protections to individual citizens, while permitting the geospatial community to grow, prosper, and bring to the market those technologies and applications that meet the economic demands of consumers and citizens.

If you have any questions, or if we can be of any assistance, please do not hesitate to contact John "JB" Byrd, MAPPS Government Affairs Manager at jbyrd@mapps.org or 703-787-6996.

Sincerely,



John M. Palatiello
Executive Director

SUBMISSION FOR THE RECORD

MCBW Minnesota Coalition for Battered Women

60 East Plato Blvd., Suite 130
St. Paul, MN 55107

Telephone: (651) 646-6177 or (800) 289-6177
Fax: (651) 646-1527

The Honorable Senate Al Franken
United States Senate
309 Hart Senate Office
Washington, DC 20515

28 May 2014

RE: SUPPORT FOR LOCATION PRIVACY PROTECTION ACT OF 2014

Dear Senator Franken:

On behalf The Minnesota Coalition for Battered Women's over 80 domestic and sexual violence advocacy programs, we applaud your dedication to ending gender violence. The Location Privacy Protection Act of 2014 ("the Act") is another example of your leadership at the forefront of efforts to improve safety for domestic violence survivors and increase community accountability.

THE PERSONAL IS POLITICAL: SURVIVOR STORIES OF CYBERSTALKING

In 2011, you listened to a brave Minnesotan's experience of domestic violence in St. Louis County, Minnesota. She shared her story: intimate partner misuse of covert technology as a tool to frighten, coerce, stalk and abuse her. You listened to her expertise on the dangers of stealth GPS "stalking apps" and have advocated for change.

As the Act has moved through the legislative process, your office has continued to consult with the true policy experts on cyberstalking: domestic abuse survivors. Unfortunately, their advice demonstrates that cyberstalking with stealth GPS "stalking apps" is a rapidly proliferating threat. Additionally, survivors have taught us that – despite the collaborative training and awareness efforts between MBCW, law enforcement and community partners – scarce resources and lack of awareness undermine our efforts. The following stories from Minnesotans demonstrate our continued struggle to meet their safety needs.

EMMA'S STORY: FROM 1,400 MILES AWAY, CYBERSTALKER FINDS HER

Emma relocated to Greater Minnesota from the other side of the country, seeking safety. Meanwhile, the man who would cyberstalk her continued to live in the state she had fled. She had not told him

where she was going. He found her anyway, shattering her sense of safety. From 1,400 miles away, he would text message her that he knew exactly where she was and who she was with. She couldn't figure out how he knew where she was. She had not seen him since she moved. Then, on a day she took a trip outside of the rural Minnesota County where she lived, he showed up out of nowhere. She was terrified. Soon after, he moved to Minnesota. The pattern of cyberstalking got worse.

With the help of a domestic violence victim advocate, Emma tried to figure out how he always knew where she was. They went to her cellphone carrier and law enforcement. Everyone said: you've got GPS tracking spyware on your phone – that's how he knows your every move. But law enforcement didn't have the technology and training to examine the phone or remove the stalking app. To be safe, she got a new phone and tried to start over. Yet, the disturbing pattern of his cyberstalking kept intruding in her life. It got so bad that the courts granted her a protective order. Nonetheless, he has continued to cyberstalk her, violating the protective order with texts that disappear as soon as she read them. She has yet to be able to prove the violations, but he somehow continues to know her every move. While she continues to safety plan with domestic violence advocates, he continues to cyberstalk her to this very day – using stealth technology to rob her privacy and peace of mind.

BETH'S STORY: CYBERSTALKING BELIEVED ONLY AFTER ATTEMPTED MURDER

Beth seemed to be a contentedly married nurse raising a beautiful son. The truth was that her husband had been abusing her for years. After law enforcement came to their home on a domestic abuse call, her husband was ordered to have no contact with her. That is when he started fighting her for custody of their son and trying to convince everyone that she was crazy and falsely alleging abuse.

Throughout that time, he would show up where she was. Sometimes publicly, but more times unknowingly. Her belongings started disappearing. When she wasn't home, she would return to find the door left slightly open or a light switch turned on when she knew she had turned it off. Her scheduled days to work were variable, and she did not always go straight home, so she really didn't feel her whereabouts were "extremely predictable." She writes: "My ex KNEW things that he shouldn't know, things that I had talked about on the phone, to my dad, to friends. They were things I knew I had never and would never discuss with my ex and it made me think I was more crazy. I thought: I can't prove anything about this, but I remember thinking: how does he know this. Why? I took my phone for service, and when I explained everything to them they went to reboot it to factory settings. It had applications running on it that they were unfamiliar with (these are guys that see applications all the time). That summer was the scariest place of my life."

Beth's reports of cyberstalking were not believed. It took him brutally bludgeoning her almost to

death for them to take her seriously. Beth survived that attack. Her ex was convicted of 1st degree attempted murder and is now serving a decades-long sentence.

Beth wonders: if there had been public awareness about the signs of cyberstalking, maybe law enforcement and the courts could have prevented a homicidal abuser from attempting to murder the mother of his child.

Beth has been working with local domestic violence advocates throughout her abuser's cyberstalking. She continues to work with them to heal from the physical and psychological trauma.

When we shared the opportunity for Beth to show her leadership in domestic violence policy advocacy, she knew that her story could help other. She is 100% supportive of the Location Privacy Protection Act and hopes that the example of her life will help pass the legislation. She hopes that the Act will stop the the marketing of stalking apps and help the criminal and civil justice systems learn to identify and effectively respond to cyberstalking victims. Beth doesn't want it to take attempted homicide for other abused women to finally be believed.

In closing, MCBW deeply appreciates your work to end gender violence and support the passage the Location Privacy Protection Act.

Sincerely,

Liz Richards
Executive Director

SUBMISSION FOR THE RECORD

THE NATIONAL CENTER FOR
Victims of Crime

June 2, 2014

The Honorable Al Franken
United States Senate
Washington, DC 20510

Dear Senator Franken:

On behalf of the National Center for Victims of Crime, I am pleased to submit this letter of support for the Location Privacy Protection Act of 2014. This legislation would close current loopholes in federal law that allow cell phone and smart phone companies to obtain and distribute customer location information without their customer's consent. This is a critical protection that should be provided to all consumers, particularly victims of stalking and domestic violence. Your bill would also make it a crime to develop or sell "apps" that facilitate stalking; any money generated from selling stalking apps can be seized by law enforcement and secured in a special fund to provide services and assistance to stalking survivors.

In January 2009, the Department of Justice report, *Stalking Victimization in the United States*, revealed that approximately 26,000 persons are victims of GPS stalking annually, including by cell phone. We believe this finding grossly underestimates the actual number of cases where victims are tracked via GPS since many victims do not know and never disclose that these devices are being used by their stalkers. Many of the tracking capabilities and applications available for cell phones and smart phones can be used against a victim without their knowledge. By enacting legislation that would ensure customers' express consent to collect and disclose location information this number could be reduced significantly.

The protection of victims' information—including their location, travel history, and online browsing history—is paramount to preventing future harm against them by stalking and abusive partners. Victims, like any users of smart phones, tablets, and other mobile devices, want to use and benefit from these sophisticated technologies. Victims of intimate partner violence and stalking, however, need to be assured that their data is private and especially not discoverable by their offender. We believe that all victims of crime and, in fact, any user of these technologies and services, deserve notice about what data is collected, where that data is stored, and, most importantly, the right and ability to opt-out of probing and location tracking features. Through this proposal, victims will gain more control over who can access their location information.

We are also grateful for your commitment to ensure that victims of stalking receive support and services. The National Center for Victims of Crime has worked for more than fourteen years to improve the nation's response to stalking victims and we strongly support the bill's provision allowing seized funds from the sale of illegal stalking apps to be used for victim assistance.

Thank you for your tireless efforts to safeguard consumers' privacy, especially victims of crime.

Sincerely,

Mai Fernandez

SUBMISSION FOR THE RECORD

June 4, 2014

The Honorable Patrick J. Leahy
Chairman
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Charles E. Grassley
Ranking Member
U.S. Senate Committee on the Judiciary
152 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Al Franken
Chairman
Subcommittee on Privacy, Technology & Law
223 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Jeff Flake
Ranking Member
Subcommittee on Privacy, Technology & Law
202 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Leahy, Senator Grassley, Senator Franken, and Senator Flake:

The National Retail Federation has deep reservations regarding S. 2171, The Location Protection Privacy Act. NRF would like to be a constructive stakeholder in a deliberative process regarding the commercial ramifications of this legislation, but we do not believe that a measure curbing cyberstalking should be accompanied with virtually unrelated legislation imposing new commercial regulations.

As the world's largest retail trade association and the voice of retail worldwide, NRF represents retailers of all types and sizes, including chain restaurants and industry partners, from the United States and more than 45 countries abroad. Retailers operate more than 3.6 million U.S. establishments that support one in four U.S. jobs – 42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy. Retailers create opportunities for life-long careers, strengthen communities at home and abroad, and play a leading role in driving innovation.

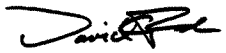
Businesses are making unprecedented investments in innovation to satisfy customer expectations in a rapidly evolving marketplace so they may build trusted relationships with their customers. Retailers' top priority is to provide our customers with a seamless, engaging, and easy shopping experience whether in store, online or mobile. Customers demand the personalization that comes with technological innovation, such as providing location-based services.

We are particularly concerned about the application of first party responsibility. The construction in this bill is in direct conflict with longstanding Federal Trade Commission policies. In examining the different relationships that exist in the marketplace, the FTC recognized that first party relationships with trusted entities are unique and distinct.

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

We urge the Committee to carefully consider the ramifications that the commercial aspects of this legislation will have and to immediately advance the domestic violence portions of the bill through the committee at this time. We believe it is important to separately consider the proposed commercial provisions and delay action on these items until all of the unintended consequences of the measure can be thoughtfully debated and addressed.

Sincerely,



David French
Senior Vice President
Government Relations

cc: Members of the Committee on the Judiciary

SUBMISSION FOR THE RECORD

OTA
Online Trust Alliance

June 2, 2014

The Honorable Al Franken, Chairman
The Honorable Jeff Flake, Ranking Member
Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law
United States Senate
223 Hart Senate Office Building
Washington, D.C. 20510

Re: Support of S. 2171; Location Privacy Protection Act of 2014

Dear Chairman Franken and Ranking Member Flake,

On behalf of the Online Trust Alliance, a global non-profit with the mission to enhance online trust and promote innovation, I am asking for your support of S. 2171, the "Location Privacy Protection Act of 2014". OTA represents over 100 organizations committed to the development and advancement of best practices, meaningful-self regulation, stewardship and balanced legislation. OTA's support of S. 2171 represents the rough consensus of our supporters.

As consumers and businesses worldwide increasingly rely on mobile devices and applications, the incidents impacting their data security and privacy continue to rise. Devices are now tethered to users with persistent identifiers and increasingly collect data on our lives. A s data collection and personal information continue to grow and provide significant benefits to consumers, so do the threats including abuse of their personal information and risk of physical harm.

OTA advocates the need to promote consumer choice and control on the collection, usage, retention and sharing of their data. While we have seen progress in self-regulatory efforts, current legislation has failed to keep pace and needs to be updated to provide protection and stem the tide of abuse.

S. 2171 is an important bill to help ensure consumer protection, while not stifling legitimate usage or innovation by business or law enforcement. It includes important changes reflecting input of industry and consumer stakeholders, notably liability cap and increased flexibility in compliance mechanisms. Equally as important are the provisions preserving the rights of State Attorney Generals in enforcing any stronger, state statute.

We endorse the Location Privacy Protection Act of 2014 and urge you to support this critical bill. Together we can increase consumer protection, promote innovation and growth of commerce.

Respectfully,

Craig D. Spiezle

Craig Spiezle
Executive Director

Kansas man convicted of stalking, choking woman in Elgin/Harry Hitzeman/DailyHerald/October 31, 2012

A 45-year-old man was convicted this week of stalking his girlfriend in Elgin and choking her when he refused to return to Kansas with him, prosecutors said.

A Kane County jury deliberated two hours before convicting Blake C. Durbin, of Maize, Kansas, of aggravated domestic battery, and two counts each of aggravated battery in a public place, stalking and domestic battery, prosecutors said.

Judge Allen Anderson will sentence Durbin on Dec. 19; he faces between three to 14 years behind bars.

"This case is an example of a domestic abuser who sees his partner as a possession and not a person. My thanks to the jury for seeing the facts as they are. This guilty verdict marks a fitting end to Domestic Violence Awareness Month," said Kane County State's Attorney Joe McMahon.

The victim left Wichita in June and arrived in Elgin to stay with a friend who had promised to help. Durbin, who authorities said physically and psychologically abused the victim, had previously given her a cellphone and had turned on the GPS on it without her knowledge.

Durbin tracked her location and traveled to Elgin, trying for days to meet with the woman by stopping by the Community Crisis Center domestic violence shelter and calling her, prosecutors said.

On July 9, Durbin went to the home on the city's southeast side where she was staying. Because kids were home at the time, the woman agreed to talk to Durbin outside in his car. Prosecutors said he became angry during the conversation, tried to strangle her and threatened to stab her. The woman's friend saw what was happening and brought her back into the home. Durbin left.

The next day, Durbin continue to call, drove by the house several times and got out to yell. He was arrested after the woman called police.

The $1 million bail for Durbin, who had been held at the Kane County jail since his arrest, was revoked after his conviction.

SUBMISSION FOR THE RECORD

Stalkers Exploit Cellphone GPS/JUSTIN SCHECK/WSJ/August 3, 2010

Phone companies know where their customers' cellphones are, often within a radius of less than 100 feet. That tracking technology has rescued lost drivers, helped authorities find kidnap victims and let parents keep tabs on their kids.

But the technology isn't always used the way the phone company intends.

One morning last summer, Glenn Helwig threw his then-wife to the floor of their bedroom in Corpus Christi, Texas, she alleged in police reports. She packed her 1995 Hyundai and drove to a friend's home, she recalled recently. She didn't expect him to find her.

The day after she arrived, she says, her husband "all of a sudden showed up." According to police reports, he barged in and knocked her to the floor, then took off with her car.

The police say in a report that Mr. Helwig found his wife using a service offered by his cellular carrier, which enabled him to follow her movements through the global-positioning-system chip contained in her cellphone.

Mr. Helwig, in an interview, acknowledged using the service to track his wife on some occasions. He says he signed up for the tracking service last year. "AT&T had this little deal where you could find your family member through her cellphone," he says. But he didn't use it to find his wife that day, he says. Mr. Helwig, who is awaiting trial on related assault charges, declined to comment further about the matter. He has pleaded not guilty.

Technology is enhancing the reach of stalkers, allowing them to take advantage of location-based social networking applications. WSJ's Andy Jordan reports.

The allegations are a stark reminder of a largely hidden cost from the proliferation of sophisticated tracking technology in everyday life—a loss of privacy.

Global-positioning systems, called GPS, and other technologies used by phone companies have unexpectedly made it easier for abusers to track their victims. A U.S. Justice Department report last year estimated that more than 25,000 adults in the U.S. are victims of GPS stalking annually, including by cellphone.

In the online world, consumers who surf the Internet unintentionally surrender all kinds of personal information to marketing firms that use invisible tracking technology to monitor online activity. A Wall Street Journal investigation of the 50 most-popular U.S. websites found that most are placing intrusive tracking technologies on the computers of visitors—in some cases, more than 100 tracking tools at a time.

The cellphone industry says location-tracking programs are meant to provide a useful service to families, and that most providers take steps to prevent abuse. Mike Altschul, chief counsel for wireless-telecommunications trade group CTIA, says recommended "best practices" for providers of such services include providing notification to the person being tracked.

Mr. Helwig's wife had received such a notification, by text message, from AT&T. A spokesman for AT&T Inc. says it notifies all phone users when tracking functions are activated. But users don't have the right to refuse to be tracked by the account holder. Turning off the phone stops the tracking.

Cellphone companies will deactivate a tracking function if law-enforcement officials inform them it is being used for stalking. Mr. Altschul says authorities haven't asked carriers to change their programs. He adds that carriers have long supported programs to give untraceable cellphones to domestic-violence victims.

In Arizona this year, Andre Leteve used the GPS in his wife's cellphone to stalk her, according to his wife's lawyer, Robert Jensen, before allegedly murdering their two children and shooting himself. Mr. Jensen says Mr. Leteve's wife, Laurie Leteve, didn't know she was being tracked until she looked at one of the family's monthly cellphone bills, more than 30 days after the tracking began. Mr. Leteve, a real-estate agent, is expected to recover. He has pleaded not guilty to murder charges, and is awaiting trial. The law firm representing him declined to comment.

In a suspected murder-suicide last year near Seattle, a mechanic named James Harrison allegedly tracked his wife's cellphone to a store. After he found her there with another man, he shot to death his five children and himself, according to the Pierce County Sheriff's Office.

Therapists who work with domestic-abuse victims say they are increasingly seeing clients who have been stalked via their phones. At the Next Door Solutions for Battered Women shelter in San Jose, Calif., director Kathleen Krenek says women frequently arrive with the same complaint: "He knows where I am all the time, and I can't figure out how he's tracking me."

In such cases, Ms. Krenek says, the abuser is usually tracking a victim's cellphone. That comes as a shock to many stalking victims, she says, who often believe that carrying a phone makes them safer because they can call 911 if they're attacked.

There are various technologies for tracking a person's phone, and with the fast growth in smartphones, new ones come along frequently. Earlier this year, researchers with iSec Partners, a cyber-security firm, described in a report how anyone could track a phone within a tight radius. All that is required is the target person's cellphone number, a computer and some knowledge of how cellular networks work, said the report, which aimed to spotlight a security vulnerability.

The result, says iSec researcher Don Bailey, is that "guys like me, who shouldn't have access to your location, have it for very, very, very cheap."

That is, in part, an unintended consequence of federal regulations that require cellphone makers to install GPS chips or other location technology in nearly all phones. The Federal Communications Commission required U.S. cellular providers to make at least 95% of the phones in their networks traceable by satellite or other technologies by the end of 2005. The agency's intention was to make it easier for people in emergencies to get help. GPS chips send signals to satellites that enable police and rescue workers to locate a person.

To a large extent, that potential has been fulfilled. Last year, for example, police in Athol, Mass., working with a cellphone carrier, were able to pinpoint the location of a 9-year-old girl who allegedly had been kidnapped and taken to Virginia by her grandmother. In December, police in Wickliffe, Ohio, tracked down and arrested a man who allegedly had robbed a Pizza Hut at gunpoint by tracking the location of a cellphone they say he had stolen.

Mr. Altschul, of the cellphone-industry trade group, says the tracking technology has been of great help to both law-enforcement officials and parents. "The technology here is neutral," he says. "It's actually used for peace of mind."

But as GPS phones proliferated, tech companies found other uses for the tracking data. Software called MobileSpy can "silently record text messages, GPS locations and call details" on iPhones, BlackBerrys and Android phones, according to the program's maker, Retina-X Studios LLC. For $99.97 a year, a person can load MobileSpy onto someone's cellphone and track that phone's location.

A memorial near Seattle for five children murdered by their father, who then killed himself, after tracking his wife by cellphone. Courtney Blethen/The Seattle Times
Craig Thompson, Retina-X's operations director, says the software is meant to allow parents to track their kids and companies to keep tabs on phones their employees use. He says the company has sold 60,000 copies of MobileSpy. The company sometimes gets calls from people who complain they are being improperly tracked, he says, but it hasn't been able to verify any of the complaints.

Installing such programs requires a person to physically get hold of the phone to download software onto it.

GPS-tracking systems provided by cellular carriers such as AT&T and Verizon Communications Inc. VZ +0.18% are activated remotely, by the carriers.

Domestic-violence shelters have learned the consequences. As soon as victims arrive at shelters run by A Safe Place, "we literally take their phones apart and put them in a plastic bag" to disable the tracking systems, says Marsie Silvestro, director of the Portsmouth, N.H., organization, which houses domestic-violence victims in secret locations so their abusers can't find them.

The organization put that policy in place after a close call. On Feb. 26, Jennie Barnes arrived at a shelter to escape her husband, Michael Barnes, according to a police affidavit filed in a domestic-violence case against Mr. Barnes in New Hampshire state court. Ms. Barnes told police she was afraid that Mr. Barnes, who has admitted in court to assaulting his wife, would assault her again.

Ms. Barnes told a police officer that "she was in fear for her life," according to court filings. The next day, a judge issued a restraining order requiring Mr. Barnes to stay away from his wife.

Later that day, court records indicate, Mr. Barnes called his wife's cellular carrier, AT&T, and activated a service that let him track his wife's location. Mr. Barnes, court records say, told his brother that he planned to find Ms. Barnes.

The cellular carrier sent Ms. Barnes a text message telling her the tracking service had been activated, and police intercepted her husband. Mr. Barnes, who pleaded guilty to assaulting his wife and to violating a restraining order by tracking her with the cellphone, was sentenced to 12 months in jail. A lawyer for Mr. Barnes didn't return calls seeking comment.

Another source for cellphone tracking information: systems meant to help police and firefighters. Some cellular carriers provide services for law-enforcement officers to track people in emergencies. Using such systems requires a person to visit a special website or dial a hot-line number set up by the carrier and claim the data request is for law-enforcement purposes.

Cellular carriers say they try to verify that callers are legitimate. An AT&T spokesman says an office is manned around the clock by operators who ask for subpoenas from law-enforcement officials using the system.

But federal law allows carriers to turn over data in emergencies without subpoenas. Al Gidari, a lawyer who represents carriers such as Verizon, says such location-tracking systems can be easy to abuse. Police, he says, often claim they need data immediately for an emergency like a kidnapping, and therefore don't have time to obtain a warrant, in which a judge must approve an information request.

In Minnesota, Sarah Jean Mann claimed last year in a county-court petition for a restraining order that her estranged boyfriend, a state narcotics agent, followed her by tracking her cellphone and accessing her call and location records through such a system. The court issued the restraining order. The boyfriend, Randy Olson, has since resigned from the police force. He didn't respond to calls seeking comment.

Mr. Gidari says law-enforcement's easy access to such data makes the systems easy to abuse. He says carriers would like to have a system in place requiring agents to get warrants. Without such a requirement, there is little carriers can do to resist warrantless requests, say Mr. Gidari and Mr. Altschul of trade group CTIA. Federal law says carriers may comply with such requests, and law-enforcement agencies have pressured them to maintain the tracking systems, Mr. Gidari says.

The easiest way for stalkers to locate a target—and perhaps the most common, say therapists who work with victims and abusers—is by using systems offered by carriers. When cellphone users sign up for a "family plan" that includes two or more phones, they have the option to contact the carrier and activate a tracking feature intended to allow them to keep tabs on their children.

The AT&T FamilyMap program, for example, is free for 30 days and requires only a phone call to activate. "Know where your kids and loved ones are at any time!" says AT&T's website. The

system is for parents, says an AT&T spokesman. He says the company hasn't received complaints about FamilyMap being used by stalkers.

The system provides an on-screen map on the smartphone or computer of the person doing the tracking. A dot on the map shows the location and movement of the person being followed. The carrier sends a text-message to the person being tracked that their phone is registered in the program.

These add-on services can be lucrative for carriers. AT&T debuted its FamilyMap system in April 2009. It charges $9.99 a month to track up to two phones, $14.99 for up to five. FamilyMap users must agree to "terms-of-use" stating that they may not use the system to "harrass, stalk, threaten" or otherwise harm anyone.

In Corpus Christi, Mr. Helwig and his wife, who had been married since early 2008, bought phones under an AT&T family plan. Mr. Helwig says he activated the feature last year. His wife says she received a text message that a tracking function had been activated on her phone, but wasn't sure how it was activated. Her husband, she says, initially denied turning on the tracking function.

She says she eventually came up with a plan to flee to the house of a family whose children she baby-sat. Her husband "had no idea where they lived" or even their names, she says. As she was packing, her husband confronted her. They argued, and, according to her statements in police reports, Mr. Helwig dragged her around by her hair.

The police came. She says she told them she didn't want them to arrest Mr. Helwig, that she simply wanted to leave. The police told Mr. Helwig to stay away from her for 24 hours, she says.

As she drove to her friend's house, she says, she made sure her phone was off so Mr. Helwig couldn't track her. But she turned it on several times to make calls. The next day, Mr. Helwig was outside in a rage, according to police reports.

Mr. Helwig forced his way into the house, pushed her to the floor, took her car keys and drove away in her Hyundai, according to police reports.

Police arrested Mr. Helwig a short distance away. Mr. Helwig, a firefighter, is facing charges of assault and interfering with an emergency call. His trial is scheduled to begin this summer.

Mr. Helwig and his wife divorced, and she left Corpus Christi. She says she doesn't want to testify against him. She says she is more careful about trusting her cellphone now.

SUBMISSION FOR THE RECORD

Accused GPS-stalker tells judge he wants to plead guilty to murder/DAN ROZEK/SunTimes/ July 18, 2011

A Canadian man charged with methodically stalking and murdering a former girlfriend after first researching whether Illinois has the death penalty did something spontaneous Monday — he told a DuPage County judge he wants to plead guilty.

But the announcement by 21-year-old Dmitry Smirnov was so surprising neither Judge Blanche Fawell nor prosecutors were ready to immediately accept his guilty plea.

Smirnov told his attorney only moments before his DuPage County court appearance that he wanted to admit to the April 13 shooting, a move that could send him to prison for life.

"I advised him not to do this, but he doesn't have to take my advice," Assistant Public Defender Steve Dalton said.

Prosecutors asked for more time to notify relatives of Smirnov's alleged victim, 36-year-old Jitka Vesel, whom authorities said briefly dated Smirnov in 2008.

Fawell rescheduled Smirnov's hearing until Friday, though Dalton plans to meet with him before then to further discuss his legal options.

A guilty plea at this stage of such a serious case is unusual, Dalton said.

Veteran prosecutor David Bayer said he can't recall a case in which a murder defendant publicly announced in court that he wanted to plead guilty.

"Not that I've handled," Bayer said.

Smirnov, who lived near Vancouver, British Columbia, allegedly researched Illinois law to determine that the state had abolished the death penalty before he drove to the Chicago area.

He allegedly glued a GPS tracking device to Vesel's car and followed her for several days before ambushing her as she left her job at a Czech fraternal organization in Oak Brook.

Smirnov is being held without bond in the DuPage County Jail.

SUBMISSION FOR THE RECORD

Stalker Victims Should Check For GPS/Francie Grace/CBS News/February 6, 2003

Connie Adams found it impossible to escape her ex-boyfriend.

He would follow her as she drove to work or ran errands. He would inexplicably pull up next to her at stoplights and once tried to run her off the highway, authorities said.

When he showed up at a bar she was visiting for the first time, on a date, Adams began to suspect Paul Seidler wasn't operating on instinct alone.

He wasn't - Seidler had installed a satellite tracking device in Adams' car, according to police in Kenosha, Wis., 30 miles south of Milwaukee.

"He told me no matter where I went or what I did, he would know where I was," Adams testified at a recent court hearing.

Police say Adams' case and several others across the country herald an incipient danger - high-tech stalking.

Just as the global satellite positioning system can help save lives, so can its abuse endanger them, advocates of stalking victims say.

"As technology advances, it's going to be almost impossible for victims to flee and get to safety," said Cindy Southworth, director of technology at the National Network to End Domestic Violence in Washington.

In the Adams case, Seidler pleaded not guilty last month to felony counts of stalking, recklessly endangering safety, burglary and a misdemeanor count of disorderly conduct. His trial is pending.

Adams does not want to speak to reporters about the case, said Susan Karaskiewicz, a Kenosha County prosecutor.

Police say Seidler put a global positioning tracking device between the radiator and grill of Adams' car. Such gadgets use a constellation of Defense Department satellites to pinpoint location and can send their coordinates via cellular networks to wireless handsets or computers.

Trucking companies use GPS systems to track of hazardous cargo and monitor drivers. Corrections authorities use them to monitor sex offenders. Hikers, boaters and motorists use GPS devices to keep from getting lost. GPS technology is also being built into cell phones to help emergency dispatchers find 911 callers. They're also being used to prevent car theft.

Southworth trains victims advocates, law enforcement and prosecutors on stalkers' use of the technology, which she says is only just beginning to be abused.

The Stalking Resource Center at the National Center for Victims of Crime has found at least one other case of a GPS system being used to stalk a victim.

In it, a Colorado appeals court in July upheld Robert Sullivan's conviction for stalking his ex-wife and installing a GPS device in her car to track her movements.

GPS is not the first technology to be misused by stalkers, who have also employed the Internet, microchip-sized cameras and even caller identification, said Southworth, though it is the most dangerous to date.

Just as she once taught victims how to block caller ID when they use the phone, Southworth now suggests victims occasionally check under their car's hood.

Police are also finding GPS devices useful. Marla Wagner, sales manager at L.A.S. Systems, the same McHenry, Ill.-based company that made Seidler's device, said the company has sold GPS systems to about 10 police departments during the last year. The Kenosha Police Department is also buying a system from L.A.S. Systems.

Tracy Bahm, the Stalking Resource Center's director, said some states are working to update their stalking statutes to include the high-tech variety.

The center typically advises states to keep their statutes broad enough to include technologies that don't yet exist.

"As society and technology evolve, stalkers will always find new ways to harass their victims," Bahm said.